Setting Up the Environment

Proprietary Notice

The manual and software contain confidential information which represents trade secrets of GE Fanuc International, Inc. and/or its suppliers, and may not be copied or disclosed except as provided in the license with GE Fanuc International, Inc. The information in this manual is subject to change without notice and should not be construed as a commitment by GE Fanuc International, Inc. GE Fanuc International, Inc. assumes no responsibility for any errors that may be in this document.

©2003 GE Fanuc International, Inc. ALL RIGHTS RESERVED.

Trademarks

©2003 GE Fanuc International, Inc. All rights reserved. Microsoft is a registered trademark of Microsoft Corporation. All other brands or names are property of their respective holders.

iFIX Version 3.5 - 07.03

Contents

Why You Should Read This Manual xiii

1. Introduction 1

SCU Overview 2

2. Getting Started 3

Hardware Requirements 4

Recommended Computers 5

Memory Requirements 6

The Hardware Key 6

Software Requirements 7

Supported Regional Settings 8

Video Drivers 9

Online Registration 10

Supported Networks 10

Supported Network Software 11

Supported File Servers 11

Optional Hardware 12

Task Overview 12

3. Working with the Hardware Key and Windows 15

Installing the Hardware Key 15

Parallel Port Hardware Key and Microsoft Windows 15

USB Port Hardware Key and Microsoft Windows 16

Recovery for Improper Installation of the Rainbow SuperPro USB Hardware Key ... 18
Troubleshooting Hardware Key Installation ... 19
Replacing Defective Hardware Keys ... 21
Using iKeyDiag ... 22
Running iKeyDiag ... 22
Using iKeyDiag Tabs ... 22
Optimizing Virtual Memory ... 23

4. Networking iFIX Nodes ... 25
Working With NetBIOS ... 25
Before You Begin With NetBIOS ... 26
Configuring NetBEUI ... 26
Working with TCP/IP ... 28
Before You Begin With TCP/IP ... 28
Configuring TCP/IP ... 31
Enabling TCP/IP in the SCU ... 34
Using Network Firewalls ... 34
Notes on Networking with Other iFIX and FIX Nodes ... 35

5. Getting Started with the SCU ... 37
Before You Begin with the SCU ... 37
Starting and Exiting the SCU ... 37
Using the SCU Toolbox ... 38
SCU File Operations ... 39
Opening a New File ... 40
Adding a File Description ... 40
Creating a Report ... 40
Configuring Directory Paths ... 40

Overview Checklist 43

6. Configuring iFIX Using the SCU 45

Configuring Local Startup Options 45

Specifying the Local Server, Local Logical, and SCU File Name 45

Running iFIX as a Service 46

Enabling the Local Node Alias Feature 48

Configuring Security 48

Configuring Network Connections 48

Configuring Protocols 48

Configuring Remote Nodes 49

Configuring LAN Redundancy 50

Configuring Network Timers 51

Configuring Alarms 51

Enabling Alarm Services 51

Customizing Alarm Services 52

Advanced Alarm Configuration 57

Editing the Alarm Area Database 58

Configuring the Auto Alarm Manager 58

Configuring the Alarm Horn 59

Configuring SCADA Servers 60

Enabling SCADA Support 60

Naming the Database 60

Configuring Drivers 61

Configuring Alarm Acknowledgement Synchronization 61

Configuring Startup Tasks 62

Running iFIX Tasks in the Background 63

Controlling SAC Startup 63

Starting I/O Drivers Automatically 64

Configuring iFIX for Relational Databases 65
Configuring the SQL Service 66
7. Using the Startup Profile Manager 67
What Exactly is a Startup Profile? 68
When Would You Use the Startup Profile Manager? 68
Understanding Startup Profiles When Upgrading from a Previous iFIX Release 69
Startup Profile Manager Basics 69
Configuring the Options for the Startup Profile Manager 70
Configuring the Default Profile 71
Security Considerations when Using the Startup Profile Manager 72
Key Combinations Available in the Startup Profile Manager 73
Working with Startup Profiles 73
General Overview of Steps for Using the Startup Profile Manager 74
Disabling or Hiding Options in the iFIX Startup Dialog Box 74
Frequently Asked Questions About the Startup Profile Manager 75
8. iFIX Startup 77
Running iFIX From the Command Line 78
iFIX Startup Options 80
Minimize After Startup 81
Show History 81
Registered Tasks 81
Shutdown 81
iFIX Background Tasks 82
9. Monitoring the Environment with Mission Control 85
Starting I/O Drivers Manually 87
Tuning the Driver's Message Rate 87
The Datascope Program 87

Starting and Stopping Historical Collect 88
Viewing SQL Statistics 88
Viewing SAC Information 88
Viewing Auto Alarm Manager Statistics 88
Viewing Alarm Acknowledgement Synchronization Statistics 89
Viewing Alarm ODBC Information 89

10. Advanced Topics 91

Understanding Network Load 91
Understanding Network Sessions 91
Understanding Data Transfer 92
Understanding Message Sizes 93
Understanding Alarm Transfer 93
Optimizing iFIX to Reduce Network Traffic 94
Working with Configurable Session Timers 94
Understanding iFIX Session Timers 95
Determining Session Timer Values 95
Configuring Session Timers 96
Working with Wide Area Networks 96
Providing Remote Access 97
Understanding Remote Access Service 98
Modifying the Registry 100
Increasing the Refresh Rate 101
RAS Examples Using iFIX Over NetBIOS 101
Network Paths 105
Integrating iFIX into Your Network 106
Disabling Connections from Unauthorized Nodes 106
Disabling Database Write Access for Unauthorized Nodes 107
SCADA Server Failover 108
Disabling the Logging of Unauthorized Writes 108

Configuring SCADA Server Failover 110

11. Troubleshooting 113

Overview 113

Understanding the Control Panel 114

Avoiding Problems 114

Computer Failures 115

Troubleshooting Computer Failures 116

Problems with Establishing or Losing Sessions 116

Troubleshooting Session Loss 117

Troubleshooting Networks 117

Troubleshooting Microsoft Networking 118

Troubleshooting NetBIOS with NBTEST 118

Exchanging Data Over NetBIOS with NBTEST Mode 1 119

Exchanging Data Over NetBIOS for an Extended Period with NBTEST Mode 2 120

Setting the Buffer Size 121

Troubleshooting TCP/IP 121

Using PING 121

Working with TCPTEST 122

Working with NETDIAG 123

Network Error Codes 124

Startup Error Codes 124

Run-time Error Codes 125

Troubleshooting the Auto Alarm Manager 126

Auto Alarm Manager Messages in Mission Control 128

Index 131

Figures

Figure 3-1: iFIX Message when No Key is Detected 19
Figure 7-1: Startup Profile Manager 67
Figure 7-2: Options Dialog Box in Startup Profile Manager 70
Figure 7-3: Default Startup Profile Dialog Box 72
Figure 8-1: iFIX Startup Dialog Box 77
Figure 8-2: iFIX Startup Dialog Box with Options Menu 80
Figure 10-1: Understanding Point to Point Communication 102
Figure 10-2: Understanding Point to LAN Communication 102
Figure 10-3: Understanding LAN to Point Communication 103
Figure 10-4: Understanding LAN to LAN Communication 104

Tables

Table 2-1: Network Software 11
Table 5-1: SCU Toolbox Buttons and Their Functions 38
Table 5-2: Path Descriptions 41
Table 6-1: I/O Control Command Line Parameters 65
Table 7-1: Startup Profile Manager Key Combinations 73
Table 7-1: Disabling or Hiding Options in the iFIX Startup Dialog Box 75
Table 8-1: Launch Command Line Options 78
Table 8-2: System Tasks 82
Table 10-1: Point to Point Communication 102
Table 10-2: Point to LAN Communication 103
Table 10-3: LAN to Point Communication 104
Table 10-4: LAN to LAN Communication 105
Table 11-1: TCPTEST Parameters 122
Table 11-2: Startup Error Messages 124
Table 11-3: Run-time Error Codes 125
Table 11-4: Troubleshooting Auto Alarm Manager Messages 128

Why You Should Read This Manual

Setting up the Environment is intended for system integrators, OEMs, and process control engineers responsible for setting up an iFIX® server or configuring their process environment. This manual assumes familiarity with Microsoft Windows and your network environment.

Reference Documents

For related information on the System Configuration Utility (SCU), refer to the following manuals:

- *Implementing Alarms and Messages*
- *Implementing Security*
- *Building a SCADA System*
- *Mastering iFIX*

1. Introduction

As you begin setting up your iFIX® environment, you have the following main tasks to complete:

- Setting up each node's hardware and operating system.
- Setting up the network you want to use.
- Configuring iFIX.

When setting up a node, you should be familiar with your hardware and Microsoft Windows operating system. If you are not, make sure you have all relevant documentation nearby for reference. Should you need to purchase one or more computers for use with iFIX, refer to the *Getting Started* chapter for iFIX requirements and recommended computers.

After setting up each node's hardware and operating system, configure the network for each computer if you plan to set up a distributed processing system. Typically, this requires you to install network interface card (also called a network adapter) and network software on each computer.

Choosing these items carefully is important to the success of your total system. The *Getting Started* chapter lists the supported networks and how to get started setting up each node for your network.

Once your nodes are connected and communicating on the network, you are ready to configure iFIX. Your main tool for accomplishing this is the System Configuration Utility (SCU). With this utility, you can specify what functions your local server performs, including:

- Where to find files.
- Where to establish security provisions.
- Which nodes to establish network connections with.
- Where to send alarm and operator messages.
- Which SCADA options to use.
- Which I/O drivers to load.
- Which database to load.
- Which programs to execute.

SCU Overview

iFIX needs two things to successfully start up:

- An SCU file.
- Local startup options.

When you start iFIX, it looks for a file that tells it how to configure the local server. This file, known as the SCU file, contains specific information about programs and options unique to that particular server.

When you start the SCU, it automatically opens the SCU file specified by the local startup options. iFIX only reads this file during startup. Any subsequent changes you make to the SCU file while iFIX is running do not take effect until you save it and restart iFIX.

For more information on the SCU file, refer to the *SCU File Operations* section. For more on local startup options, refer to the *Configuring Local Startup Options* section.

2. Getting Started

Before you start setting up your iFIX environment, complete the following tasks:

- Identify the computers that will function as your View clients, SCADA servers, and development workstations.
- Identify which nodes will be networked, if any.
- Decide if you want to use a file server to share alarm area databases, or SCU, security, historical, or recipe files.
- Identify the computer that will function as the file server if you decide to use one.
- Make sure that you have a Windows user account that is a member of either the Administrators group or the Power Users group.

  Intellution recommends that all iFIX users be a member of either the Administrators or the Power Users group. This setting allows users full access to all iFIX applications, such as the iFIX Sample System, the SCU, and the Security Configuration tool. It is possible to have iFIX users be part of the Users group, but such users do not have access to these iFIX applications, or any other application that needs to create or modify files.

  Terminal Server clients must be a member of at least the Power Users group. Refer to the *Using Terminal Server* manual for more information.

Hardware Requirements

The minimum iFIX hardware requirements are:

- A Pentium II-based 266 MHz computer. For optimum performance, Intellution recommends a Pentium 4-based 1 GHz computer. For a list of machines tested by Intellution, refer to the *Recommended Computers* section.

- A minimum of 96MB RAM for SCADA servers and iClients. Refer to the *Memory Requirements* section for more information.

- 120MB of free hard drive space to install a typical iFIX system, including pictures, databases, alarm files, and other data files.

  iFIX alarm and historical data files grow dynamically. If you plan to perform extensive alarm or data collection on a node, you may need more disk space on that particular node.

  Other Intellution® products, such as iDownTime, iHistorian, and infoAgent, impose additional requirements. Refer to the appropriate electronic manual for specific system requirements.

- A CD-ROM drive.

- NETBIOS-compatible or TCP/IP-compatible network interface adapter for network communication and certain I/O drivers.

  NOTE: *Because Microsoft does not support NetBIOS on Windows XP or Windows Server 2003, iFIX installed on Windows XP or Windows Server 2003 also does not support NetBIOS.*

- One parallel or free direct-connect USB port. Some touch screens, pointing devices, and I/O drivers require a serial port. Additional ports for I/O hardware should be ordered with the computer.

- SVGA or better color graphics monitor and a 100% IBM-compatible, 24-bit graphics card capable of 800x600 resolution and at least 65,535 colors.

- Two-button mouse or compatible pointing device (such as a touch screen).

Recommended Computers

iFIX has been tested by Intellution® on the following machines that were running Windows NT, Windows 2000, Windows XP, and Windows Server 2003:

- Compaq Deskpro
- Compaq EVO D500 (Desktop 500 Minitower)
- Dell Dimension
- Dell Optiplex GX1
- Dell Optiplex GX110
- Dell Optiplex GX200
- Dell Precision 340
- Dell Precision 530 Dual Xeon
- Dell Precision Workstation 420MT
- Dell Precision Dual
- Gateway 8400 Server (Quad Processor)
- IBM NetVista
- Micron Millennia
- Stratus® ftStratus® 3300

While Intellution cannot guarantee the integrity of any computer, our testing has shown a higher potential for problems with the economy lines of computers on the market. Because of these problems, Intellution does not recommend the use of value or economy type computers with iFIX. Instead, Intellution recommends you invest in the higher end (premier) line of computers when purchasing computer hardware.

Memory Requirements

iClients and SCADA nodes require at least 96MB RAM. This configuration provides enough memory to run iFIX applications. Intellution recommends at least 128MB RAM.

NOTE: *As more applications run simultaneously on a SCADA server, performance decreases. Whenever possible, run additional applications on different computers.*

If the size of your process database is over 1MB, add 1 megabyte of memory for each megabyte of database size. For example, if your database is 2MB in size, your SCADA server requires 98MB minimum (96+2=98).

The Hardware Key

You are required to use a hardware key to run iFIX. The hardware key:

- Controls and enables software options available to your installation, as requested by you.

- Uses a utility to electronically reprogram options you choose to upgrade or change. Consequently, you are no longer required to exchange hardware keys for version updates or option changes.

Additionally, two hardware keys are offered, one that supports parallel port configurations, and one that supports USB port configurations.

iFIX runs in demo mode for two hours if the key is not installed. Hardware keys from version 2.5 and older will not work. You can exchange the older key by contacting your iFIX sales representative. You will need to use iKeyUpdate to upgrade your hardware keys from version 2.6 and later.

Be sure to file your hardware key packing slip in a safe location. The codes on this slip are necessary for Intellution to quickly duplicate the key in case it is damaged or misplaced. You can verify that your serial number matches the serial number on the hardware key packing slip by using the iKeyDiag utility to detect and display your hardware key settings. For more information, see *Using iKeyDiag*.

Software Requirements

The minimum iFIX software requirements are:

- One of the following operating systems:
  - Microsoft® Windows® NT v4.0, with Service Pack 6a.
  - Microsoft® Windows® 2000, Professional or Advanced Server Edition, with Service Pack 2 or greater recommended.
  - Microsoft® Windows® XP Professional. Since Windows XP has continuous updates, you should run the Windows update feature to get the latest software.
  - Microsoft® Windows® Server 2003, Standard or Enterprise Edition. Since Windows Server 2003 has continuous updates, you should run the Windows update feature to get the latest software.
- Network interface software for network communication and certain I/O drivers.
- An I/O driver for SCADA servers. Intellution supplies I/O drivers for many programmable controllers or you may purchase a driver separately. Be certain that the I/O driver you purchase is compatible with your hardware. Contact your Intellution Sales Representative or visit the Intellution web site at http://www.gefanucautomation.com/products/fixiodrivers/default.asp for the latest list of drivers and supported hardware.
- Internet Explorer v5.5 or higher

Supported Regional Settings

iFIX supports the following regional settings available in the Windows Control Panel:

- Decimal symbol - one character
- Digit grouping symbol
- List separator - one character
- Time style
- Time separator
- Short date style
- Date separator

NOTE: *The decimal symbol and the digit grouping symbol cannot be the same character. Also, the time separator and the date separator cannot be the same character.*

Formatting the Time and Date

Avoid changing the time style or short date style in regional settings to values that are outside of the standard styles provided. Changing these values to non-standard styles may result in improperly formatting times and dates in some parts of iFIX.

iFIX supports the following short date formats, some of which may not be available in certain language versions of Microsoft Windows:

- dd/mm/yy, or dd/mm/yyyy
- dd/yy/mm, or dd/yyyy/mm
- mm/dd/yy, or mm/dd/yyyy
- mm/yy/dd, or mm/yyyy/dd
- yy/dd/mm, or yyyy/dd/mm
- yy/mm/dd, or yyyy/mm/dd

Formatting the Regional Language Setting

Avoid changing the language setting once a timer has been used in a schedule. If changed, the date always reverts to 30/12/99, regardless of what you set the start time to be.

Setting the System Default Locale

The selected locale must be set as the system default.

Video Drivers

After much testing, Intellution has found that some video drivers have unique problems which are only apparent when using these drivers. Additionally, Intellution has found that many problems with video drivers occur in both iFIX applications and common applications (such as Excel and Word).

If you are experiencing problems with your video driver, try using it in a different mode to find out if the problem is unique to a specific configuration.

Using Third-Party Video Drivers

If you need to use a third-party driver, please use the following guidelines to resolve any problems you may experience:

- Contact the manufacturer to ensure you have the latest version of the video driver. Intellution has found, after extensive testing, that the latest version of third-party video drivers can fix some problems.
- If the latest version of the video driver does not fix the problem, notify the video driver manufacturer to see if they are aware of the problem.
- If all else fails to resolve the problem, contact Intellution Technical Support.

Online Registration

You can register iFIX online during the product installation. However, you can also register the product online after you have installed iFIX.

To register iFIX online:

[1] Select Intellution iFIX WorkSpace Help from the WorkSpace Help menu, and then select Intellution On the Web.

[2] From the sub-menu that appears, select Register Online.

[3] Enter the appropriate fields on the registration form, and click Next until all pages are completed.

Supported Networks

If you decide to implement a networked iFIX system, make sure that all nodes are using compatible network configurations. Currently, iFIX supports the NetBIOS and TCP/IP interfaces for peer-to-peer communications in Windows NT and Windows 2000. Under Windows XP and Windows Server 2003, iFIX supports only TCP/IP interfaces. Intellution has tested and recommends 3COM plug-in boards and built-in network adapters from Compaq, Dell, and Gateway.

If you have difficulty networking your computer, refer to the chapter *Troubleshooting* to pinpoint and resolve your problems.

Supported Network Software

Intellution recommends and supports the network software that is provided by Microsoft Windows. The following table lists the supported software that provides the network interface and the sections that contain setup instructions for the software. The software can be combined with Compaq, Dell, or Gateway network adapters to provide a complete networking solution.

Table 2-1: Network Software

For the network software...	**Refer to the section in the *Setting Up the Environment* manual...**
NetBIOS	*Working With NetBIOS*
TCP/IP	*Working with TCP/IP*

Supported File Servers

Intellution supports using a file server to store System Configuration Utility, alarm area database, security, historical, and recipe data files and file server-based View clients. iFIX does not require a file server.

The following file servers are recommended:

- Microsoft Windows NT Server.
- Microsoft Windows 2000 Server/Advanced Server.
- Microsoft Windows Server 2003
- Novell NetWare. If you use a NetWare file server, Intellution recommends that you use Microsoft's Client Service for NetWare on your iFIX node.

Refer to your file server documentation for installation and configuration instructions.

If a file server becomes unavailable and an iFIX node attempts to access a file, you may experience no response, slow response, or time-outs. These conditions are a result of continuously polling all available drives while it waits for a response from the file server. It is recommended that you store a backup copy of the files you need on the local node. Intellution does not recommend using the file server for files if it is susceptible to failure.

Optional Hardware

iFIX supports the following optional hardware. You may want to purchase one or more of these items to enhance your iFIX system.

- A Microsoft-supported touch screen or other pointing device.
- A DigiBoard™ to provide your computer with up to 9 serial ports. If you are using multiple I/O drivers or multiple ports for one I/O driver, you may require the use of a DigiBoard. Intellution has tested and supports the Digichannel PC/8E.

Task Overview

When you are ready to begin setting up your iFIX environment, use the following steps to set up your nodes:

[1] Set up each computer you require. Use the section *Hardware Requirements* as a guide and refer to the user manual that accompanies each computer for detailed setup information.

[2] Install and optimize Microsoft Windows on each computer as needed. Also make sure you create a login account with administrator rights so you can install iFIX later. For instructions on optimizing Windows, refer to the chapter *Working with the Hardware Key and Windows.*

[3] Set up the network adapters and network software required for each computer. Refer to the chapters *Networking iFIX Nodes* and *Advanced Topics* for more information.

[4] Install the hardware key and any other hardware you may have purchased. Refer to the section *Installing the Hardware Key* for instructions on attaching the key to your computers. For information on installing other hardware, refer to the hardware installation guide that accompanies it.

[5] Install and configure the iFIX on each computer. Make sure that the user installing iFIX is a member of the Administrators Windows group. Refer to the chapter *Configuring iFIX Using the SCU* for more information on configuring iFIX.

3. Working with the Hardware Key and Windows

As you set up each computer in your iFIX environment, you need to install a hardware key and optimize Windows for use with iFIX. This chapter describes how to complete these tasks.

This chapter also contains information about replacing defective hardware keys and using the iKeyDiag utility.

Installing the Hardware Key

A hardware key is included with your iFIX software. You must install your hardware key in order to access all the components of the iFIX software you purchased. The following sections provide procedures for installing your hardware key. Follow the appropriate procedures for your key type.

Parallel Port Hardware Key and Microsoft Windows

Intellution supports the installation of a parallel port hardware key on systems running Microsoft Windows.

To install the parallel port hardware key:

[1] Power off the computer and all peripheral devices before installing the hardware key; it is sensitive to static electricity.

[2] Remove any connections to your computer's parallel port.

[3] Secure the hardware key in the parallel port and tighten the screws.

IMPORTANT: *Do not remove the hardware key from your node while iFIX is running. If you do, iFIX features will shut down and you will need to restart iFIX. You may also damage the hardware key if you remove it while iFIX is running.*

[4] If you had any equipment connected to your parallel port, re-connect to the back of the hardware key.

USB Port Hardware Key and Microsoft Windows

GE Fanuc supports the installation of the USB port hardware key only on systems running Windows 2000, Windows XP, or Windows Server 2003.

At this time, GE Fanuc does not support USB keys connected through an external USB hub.

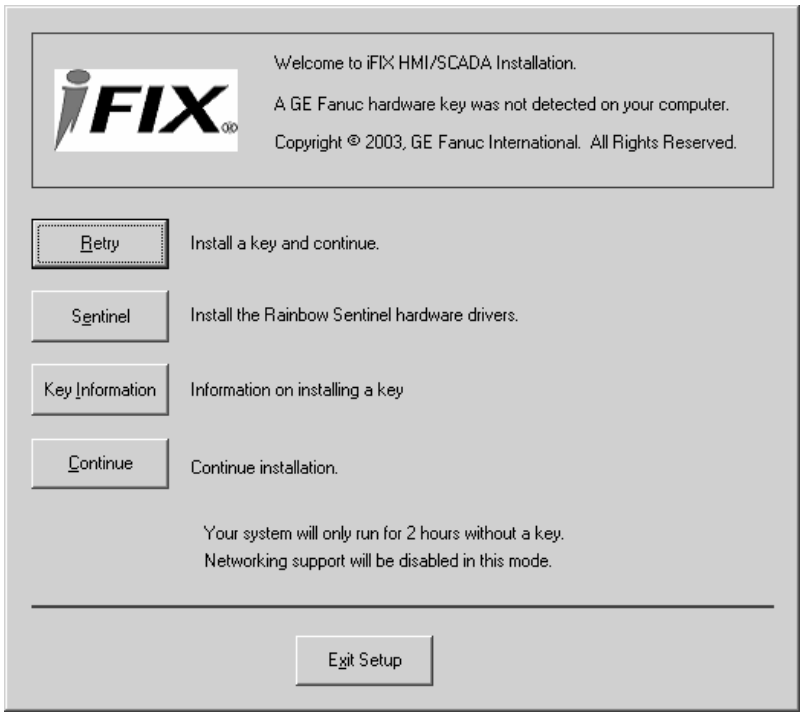
IMPORTANT: *If you are using a Rainbow/SuperPro Key from a Previous iFIX release, do not install the hardware until after you install the iFIX product. If you accidentally installed the hardware first, follow the steps in the Recovery for Improper Installation of the Rainbow SuperPro USB Hardware Key section.*

To install the USB port hardware key license:

[1] Run iDemo.exe to begin the iFIX installation process. You can find this file on the iFIX installation CD in the DemoShield folder.

[2] Click Install iFIX 3.5.

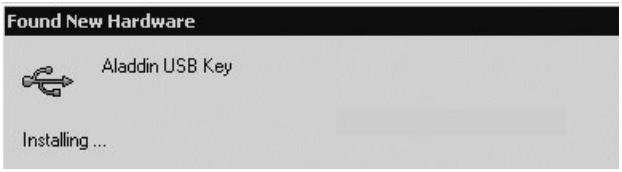
[3] The following installation dialog box appears.


Welcome to iFIX HMI/SCADA Installation.
A GE Fanuc hardware key was not detected on your computer.
Copyright © 2003, GE Fanuc International. All Rights Reserved.
Retry
Install a key and continue.
Sentinel
Install the Rainbow Sentinel hardware drivers.
Key Information
Information on installing a key
Continue
Continue installation.
Your system will only run for 2 hours without a key.
Networking support will be disabled in this mode.
Exit Setup

[4] Insert your USB hardware key in the appropriate port.

IMPORTANT: *If you are using a Rainbow/SuperPro Key from a previous iFIX release, you also need to install the Sentinel driver so that iFIX recognizes this key. To install this driver, click the Sentinel button on the installation screen.*

[5] A message box, similar to the following figure, appears as the hardware key installs:

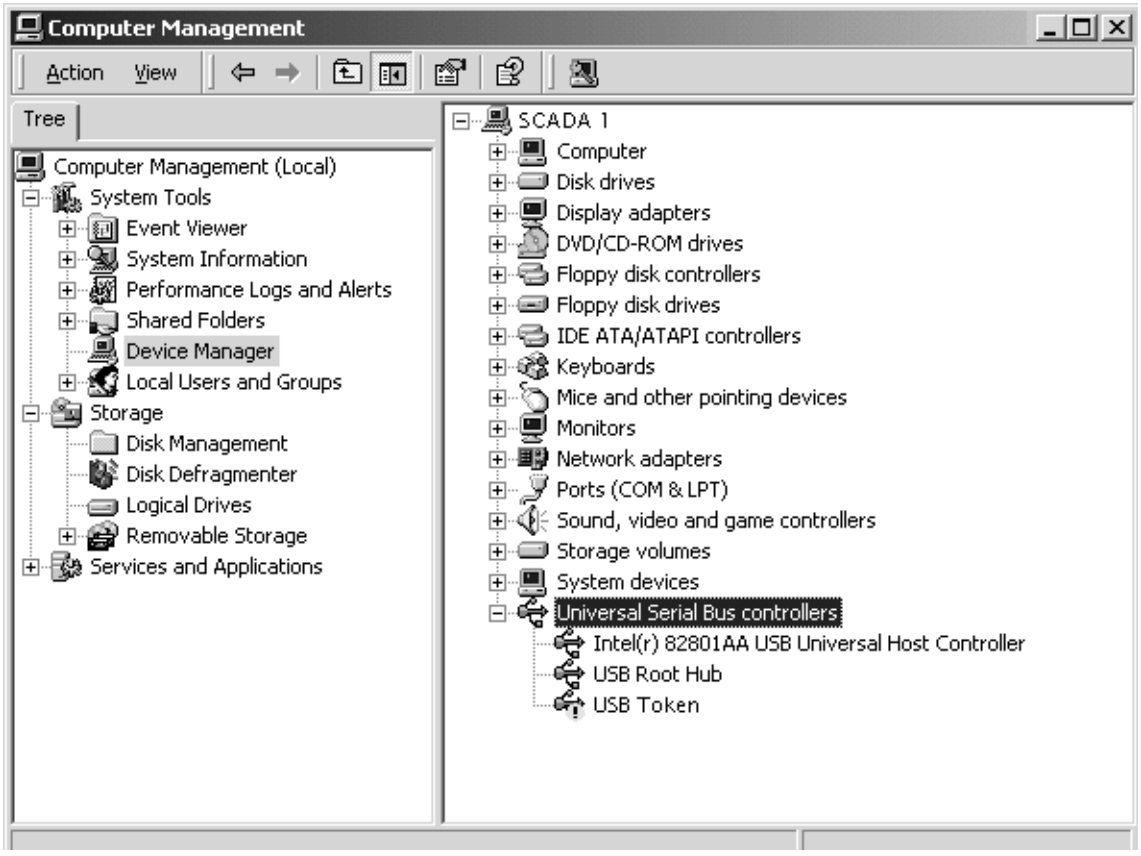


[6] Once the hardware installation and licensing is complete, click Retry in the iFIX installation dialog box.

Recovery for Improper Installation of the Rainbow SuperPro USB Hardware Key

If you inserted the Rainbow SuperPro USB hardware key prior to installing the Sentinel System Driver, a dialog box requesting USB drivers appears. Cancel this dialog box, and then follow these steps to uninstall the incorrectly installed USB hardware key:

[1] Right-click the My Computer icon on your desktop and select Manage from the right-click menu. The following dialog box appears:



[2] Select Device manager from the System Tools tree.

[3] Select Universal Serial Bus controllers from the right pane of the Computer Management dialog box.

[4] Right-click USB Token. Choose Uninstall from the right-click menu.

[5] Click OK to confirm uninstall.

[6] Remove the USB hardware key from your computer and reboot your machine.

[7] Continue the correct installation using procedures from the *USB Port Hardware Key and Microsoft Windows* section of this manual.

Troubleshooting Hardware Key Installation

If the hardware key does not install properly, you may find that even though you have followed the installation directions for your hardware key, you see the following message from iFIX:

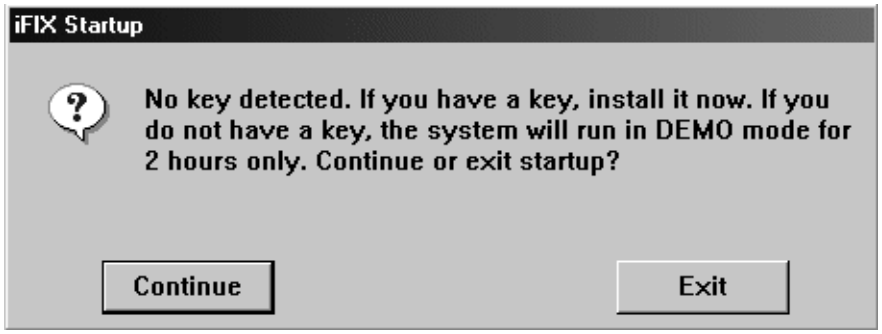

iFIX Startup
No key detected. If you have a key, install it now. If you do not have a key, the system will run in DEMO mode for 2 hours only. Continue or exit startup?
Continue
Exit

Figure 3-1: iFIX Message when No Key is Detected

First, check to see that your hardware key is firmly attached. Next, uninstall and reinstall the driver for the hardware key. If this driver has been incorrectly uninstalled, it may cause trouble.

Troubleshooting the New Aladdin/HASP USB Key...

If the Aladdin/HASP USB key does not appear to be working, you can reinstall the Intellution Licensing to recover from the improper install. When the Aladdin/HASP key is not communicating correctly, you will notice that the indicator light at the end of the key is off.

To reinstall the Intellution Licensing, follow these steps:

[1] Reinstall the Intellution Licensing by clicking the Setup.exe file in the License folder on the iFIX product installation CD.

[2] Click Finish when the licensing install completes.

Troubleshooting the Rainbow SuperPro USB Key from a Previous iFIX Release...

If the Rainbow/SuperPro key does not appear to be working, you can uninstall the Sentinel System Driver to recover from the improper install.

To uninstall the Sentinel System driver for the Rainbow/SuperPro key:

[1] Double-click Add/Remove Programs in your Control Panel.

[2] Select the Sentinel System Driver from the list of currently installed programs and click Remove.

[3] Run the setup.exe file from the following directory on your iFIX Installation disc:

\SentinelDriver

If you see the message in *Figure 3-1* and do not see Sentinel System Driver in your list of currently installed programs, you may have implemented the Windows XP or IBM rollback feature to restore your registry to a previous state. This process does not remove files, and the Sentinel System Driver will not install over existing files. You will need to remove the file manually.

To remove the file manually:

- Delete the following file:

  WINNT\system32\drivers\sentinel.sys

To reinstall the Sentinel System Driver:

[1] Click Sentinel button from the install screen.

[2] After the driver installs, plug the key into the USB port.

Replacing Defective Hardware Keys

Defective hardware keys cause iFIX to generate the following error message when it starts or when you start an application:

```
ERROR - MISSING SECURITY KEY OR FILE
```

The message may also indicate that the hardware key is not securely installed. Be sure to check the connection before assuming your hardware key is defective.

You can also tell if a hardware key is invalid by running the iKeyDiag.exe application in the Dynamics folder (the folder where you installed iFIX). The Licensing Info tab for the KeyDiag utility indicates whether the license is not current or invalid.

Intellution replaces defective keys as quickly as possible. To obtain a replacement hardware key:

- Call your local Intellution technical support representative. The support representative will instruct you to FAX a completed copy of a Merchandise Return Authorization form. On receipt of the form, Intellution can program a new hardware key and send it to you overnight.

- When you receive the hardware key, you must return the old one along with a copy of the form sent with the new hardware key. Intellution reserves the right to invoice for defective hardware keys that are not returned.

Using iKeyDiag

iKeyDiag is a diagnostic tool that provides technical support personnel with information about your iFIX hardware key. This tool is located in the Dynamics directory of your iFIX node.

Running iKeyDiag

You can run iKeyDiag in the following three ways:

- Select Run from the Start menu, enter ikeydiag in the Open field of the Run dialog box, and then press the Enter key.
- Double-click the iKeyDiag.exe file in the Dynamics directory.
- Start iFIX. Select About Intellution iFIX WorkSpace from the Intellution iFIX WorkSpace Help located in the Help menu, and click the Launch iKeyDiag button.

The iKeyDiag dialog box consists of a series of tabs. Each tab contains fields that provide information about the setting of your iFIX hardware key. You can use the common OK or Cancel buttons to close the dialog box from any tab.

IMPORTANT: *If you run iKeyDiag while running the Sample System, the information displayed will reflect settings on a demo key, rather than the actual settings of your hardware key. To see your hardware key settings, close the Sample System before running iKeyDiag.*

Using iKeyDiag Tabs

The following list provides a brief description of the information displayed on each iKeyDiag tab.

Licensing Info – Customer name, Order Number when hardware key was last programmed, unique Identification Number, Key Style (USB port or parallel port), Key Type, Expiration Date, and Key Properties.

Other Options – Any other iFIX run time and baseline options.

SCADA – SCADA settings enabled on your system.

Drivers – DRIVER settings enabled on your system.

iClientTS – Indicates if the key is enabled for Terminal Server, and, if so, the maximum number of concurrent Terminal Server connections allowed.

FIX BOS – FIX BOS components enabled on your system.

infoAgent – iBatch components enabled by your hardware key.

iBatch – iBatch components enabled by your hardware key.

iHistorian – iHistorian settings, such as iHistorian Server, number of points, and whether you can modify iHistorian data.

OEM – Indicates if the ROC driver is enabled, the number of ROC licenses, and any OEM options you may have purchased from other manufacturers that are enabled with the hardware key.

License Display – A snapshot of all enabled settings and other information at a particular date and time. You have the option to save this information to a file called key_report.txt, located in the \Dynamics\App folder.

NOTE: *Since the key_report.txt file is used only by Intellution Technical Support, it will not be translated, and its content will remain in English.*

Optimizing Virtual Memory

Through the use of paging files, Windows allocates space on your hard drive for use as if it were actually memory. This space is known as virtual memory. After you install Windows, be sure to optimize the virtual memory for use with the iFIX. The following sections describe how to optimize virtual memory in Windows to achieve maximum performance from iFIX.

To optimize the virtual memory paging file for iFIX in Windows:

[1] Double-click the System icon in the Windows Control Panel.

[2] In the Windows NT System Properties dialog box, click the Performance tab.

In the Windows 2000 System Properties dialog box, click the Advanced tab, then select Performance Options.

In the Windows XP System Properties dialog box, click the Advanced tab, then in the Performance group box, select Settings. In the Performance Options dialog box, click the Advanced Tab.

In the Windows Server 2003 System Properties dialog box, click the Advanced tab, then select Performance Options.

[3] Select Change in the Virtual Memory group box.

[4] Enter a value equal to three times your physical memory in the Initial Size field.

[5] Enter a value equal to three times your physical memory in the Maximum Size field.

[6] Select Set.

[7] Click OK to save the changes and exit the dialog box.

NOTE: *If the paging file is set to grow dynamically, your system may experience severe performance problems during runtime. To ensure optimal performance, be sure that the Initial Size and Maximum Size of the paging file are the same so that the paging file does not grow dynamically.*

4. Networking iFIX Nodes

This chapter describes how to set up network hardware and driver software for Ethernet adapters. The chapter also describes how to set up NetBEUI and TCP/IP protocols for iFIX nodes.

In general, you can accomplish these tasks as follows:

[1] Select the network protocol you want to use.

[2] Configure the network protocol for each computer in the network.

When you finish, make sure each computer can communicate with your network before proceeding. If it cannot, refer to the chapter *Troubleshooting* to resolve any difficulties you experience.

Working With NetBIOS

When running on Windows NT or Windows 2000, iFIX supports the NetBIOS interface over the Microsoft NetBEUI (NetBIOS Extended User Interface) protocol using Intel Ethernet and 3COM Ethernet network adapters. However, Microsoft discontinued support for NetBEUI in Windows XP and Windows Server 2003. For more information on the discontinued support, beginning with Windows XP, refer to Microsoft Knowledge Base article Q306059.

Refer to the section *Configuring NetBEUI* for information on configuring Windows NT with Microsoft's NetBEUI, and the section *Configuring NetBEUI for Windows 2000* for more information on configuring Windows 2000 with Microsoft's NetBEUI. For information on configuring FIX to run over the TCP/IP protocol, refer to the section *Working with TCP/IP*.

Before You Begin With NetBIOS

To use Windows NT or Windows 2000 with NetBEUI as the NetBIOS implementation, make sure you have the following components:

- Windows NT 4.0 or Windows 2000 installation disks or CD-ROM and documentation.
- Network adapter, drivers, and cabling.

For more detailed information on Windows NT, refer to your Windows NT documentation and the Microsoft Windows NT Resource Kit. For detailed information on Windows 2000, consult your Windows 2000 documentation.

Configuring NetBEUI

You can configure NetBEUI with the Windows NT or Windows 2000 Network control panel. Microsoft recommends that you use the Network control panel for all network configuration tasks rather than manually editing the registry.

NOTE: *Have the Windows NT or Windows 2000 disks or CD-ROM available. You may need them to configure NetBEUI.*

Configuring NetBEUI for Windows NT

To set up NetBEUI for Windows NT:

[1] Open the Windows NT Control Panel and double-click the Network icon, shown below:

The Network dialog box appears.

[2] Use the following table to verify all the components for NetBEUI are installed.

Select the tab…	To verify that the…
Services tab	NetBIOS interface is installed.
Protocols tab	NetBEUI protocol is installed.
Adapters tab	Network adapter driver required for the network adapter hardware is installed.

If all of the above network components are installed, skip to step 6 of this procedure.

[3] If a driver for the network adapter is not currently installed:

[a] Select the Adapters tab.

[b] Click the Add button.

[c] Select your network adapter type from the Select Network Adapter dialog box.

[d] Click OK to save your changes and return to the Network dialog box.

[4] If the NetBIOS interface is not currently installed:

[a] Select the Services tab.

[b] Click the Add button.

[c] Select NetBIOS Interface from the Select Network Service dialog box.

[d] Click OK to save your changes and return to the Network dialog box.

[5] If the NetBEUI protocol is not currently installed:

[a] Select the Protocols tab.

[b] Click the Add button.

[c] Select NetBEUI Protocol from the Select Network Protocol dialog box.

[d] Click OK to save your changes and return to the Network dialog box.

[6] Restart the computer. The computer is now ready to run iFIX over the NetBEUI protocol.

Configuring NetBEUI for Windows 2000

To configure NetBEUI for Windows 2000:

[1] Open the Windows 2000 Network and Dial-Up Connections in the Control Panel.

[2] Right click on the Local Area Connection icon and select properties from the right-click menu. The Local Area Connection Properties dialog box appears.

[3] From the General tab, verify that all the components for NetBEUI are installed: NetBIOS interface, NetBEUI Protocol, and a network adapter driver required for the network adapter hardware.

[4] Consult your Windows 2000 documentation for information about installing missing components.

Working with TCP/IP

iFIX can use TCP/IP instead of NetBIOS to provide connectivity for your nodes. Microsoft's TCP/IP is available for Windows NT, Windows 2000, or Windows XP nodes and is built into the operating system.

Before You Begin With TCP/IP

To use Windows NT, Windows 2000, Windows XP, or Windows Server 2003 with TCP/IP, make sure you have the following components:

- Microsoft Windows installation disks or CD-ROM and documentation.
- Network adapter, drivers, and cabling.

For more detailed information on Windows NT, refer to your Windows NT documentation and the Microsoft Windows NT Resource Kit. For detailed information on Windows 2000, Windows XP, or Windows Server 2003 refer to the Microsoft online Help that came with your operating system.

In addition to the components you need to get started, you need do the following:

- Map the names of each SCADA server IP addresses.
- Verify the communication ports that FIX will use.
- Configure TCP/IP
- Enable the TCP/IP protocol in the SCU.

The following sections provide guidelines for completing these tasks. Refer to your TCP/IP manuals for additional configuration information.

Mapping IP Addresses

To use a TCP/IP network with iFIX, each SCADA server must be mapped to unique IP addresses. This process is called *name resolution*, and TCP/IP vendors handle this in many different ways. You need to decide which method of name resolution is appropriate for your site. This section provides guidelines to help you reach that decision.

TCP/IP software can handle name resolution using the following:

- A local HOSTS file.
- DNS (Domain Name System).
- DHCP/WINS (Dynamic Host Configuration Protocol and Windows Internet Naming Service).

Intellution recommends using a local HOSTS file since this method has provided the highest reliability during our testing. More information on using a local HOSTS file is included in the section *Using a Local HOSTS File*.

If your company currently uses DNS servers, this option can be implemented since DNS servers are based on HOSTS files.

Using a Local HOSTS File

The HOSTS file provides mapping between node names and IP addresses. This text file is stored locally on each node. The contents of the HOSTS file should be identical on each node in your TCP/IP network. All FIX SCADA servers must be in the HOSTS file.

The syntax is as follows:

```
address       HOSTNAME
```

Address — defines the IP address of the node.

Hostname — defines the iFIX node name, as specified in the SCU. The node name must be in uppercase and is limited to eight characters.

An example of an entry in the HOSTS file is as follows:

```
198.212.170.4       SCADA01
```

You can also provide an alias name for the host name as an optional third parameter.

Using DNS Servers

A DNS server is a HOSTS file stored on a server. This configuration is easier to administer than local HOSTS files since any changes to the HOSTS file need to be made only once. However, a single DNS server can be a single point of failure should it fail to respond. If avoiding a single point of failure is important to you, consider doing one of the following:

- Reverting back to local HOSTS files.
- Implementing redundant DNS servers.

Using DHCP/WINS

When using iFIX with DHCP, you also need to use WINS. The local host name must be the same as the iFIX node name. Refer to your Microsoft documentation for more information on setting up DHCP and WINS.

Verifying Port Assignments

By default, iFIX uses the following port:

```
FIX2010/tcp
```

You should not have to change this setting. If the number is used by another application on your node, you must edit or create a SERVICES file. The SERVICES file defines the port used by each TCP/IP application.

To define unique port numbers for iFIX, refer to your TCP/IP manuals for instructions on locating and editing the SERVICES file. Make sure, when you edit the file, you enter a unique port number for iFIX or change the port number of the conflicting application.

Configuring TCP/IP

You can configure TCP/IP with the Windows Network control panel. Microsoft recommends that you use the Network control panel for all network configuration tasks rather than manually editing the registry.

NOTE: *Have the Microsoft Windows disks or CD-ROM available. You may need them to configure TCP/IP.*

Configuring TCP/IP for Windows NT

To set up TCP/IP for Windows NT:

[1] Open the Windows NT Control Panel and double-click the Network icon, shown below:

The Network dialog box appears.

[2] Use the following table to verify all the components for TCP/IP are installed.

Select the tab…	To verify that the…
Protocols tab	TCP/IP protocol is installed.
Adapters tab	Network adapter driver required for the network adapter hardware is installed.

If both of the above network components are installed, skip to step 5 of this procedure.

[3] If a driver for your network adapter is not currently installed:

[a] Select the Adapters tab.

[b] Click the Add button.

[c] Select the network adapter type from the Select Network Adapter dialog box.

[d] Click OK to save your changes and return to the Network dialog box.

[4] If the TCP/IP protocol is not currently installed:

[a] Select the Protocols tab.

[b] Click the Add button.

[c] Select TCP/IP Protocol from the Select Network Protocol dialog box.

[d] Click OK to save your changes and return to the Network dialog box.

[5] Select TCP/IP Protocol from the Protocol tab and click the Properties button. The Microsoft TCP/IP Properties dialog box appears.

If you want to use DHCP:

[a] Select the Obtain an IP Address from a DHCP Server option button.

[b] Refer to the section *Using DHCP/WINS*.

[c] Skip steps 6 and 7 of this procedure.

[6] If it is not already selected, select the Specify an IP Address option button.

[7] Enter your IP address and Subnet Mask into their respective fields. Ask your network administrator for these values. Once you have entered these values, click OK to save your changes and return to the Network Settings dialog box.

[8] Click OK in the Network dialog box to save your changes and exit from the Network Control Panel.

[9] Restart the computer. The computer is now ready to run iFIX over the TCP/IP protocol.

Configuring TCP/IP for Windows 2000

To configure TCP/IP for Windows 2000:

[1] Open the Windows 2000 Network and Dial-Up Connections in the Control Panel.

[2] Right-click on the Local Area Connection icon and select properties from the right-click menu. The Local Area Connection Properties dialog box appears.

[3] From the General tab, verify that all the components for TCP/IP are installed: TCP/IP Protocol and a network adapter driver required for the network adapter hardware.

[4] Consult your Windows 2000 documentation for information about installing missing components.

Configuring TCP/IP for Windows XP

To configure TCP/IP for Windows XP:

[1] Open Windows XP Network Connections in the Control Panel.

[2] Right-click on the Local Area Connection icon and select properties from the right-click menu. The Local Area Connection Properties dialog box appears.

[3] From the General tab, verify that all the components for TCP/IP are installed: TCP/IP Protocol and a network adapter driver required for the network adapter hardware.

[4] Consult your Windows XP documentation for information about installing missing components.

Configuring TCP/IP for Windows Server 2003

To configure TCP/IP for Windows Server 2003:

[1] Open Windows Server 2003 Network Connections in the Control Panel.

[2] Right-click on the Local Area Connection icon and select properties from the right-click menu. The Local Area Connection Properties dialog box appears.

[3] From the General tab, verify that all the components for TCP/IP are installed: TCP/IP Protocol and a network adapter driver required for the network adapter hardware.

[4] Consult your Windows Server 2003 documentation for information about installing missing components.

Enabling TCP/IP in the SCU

You can switch between NetBIOS and TCP/IP protocol with the SCU.

Using Network Firewalls

iFIX does not support using network firewalls. If two or more View clients attempt to connect to a SCADA server which is behind a firewall, the View client will not remain connected. One clue that the SCADA server is behind a firewall is that the client nodes will connect and disconnect continuously.

This situation occurs because the iFIX TCP/IP implementation is connection-oriented while the SCADA server keeps track of connections by IP address. The problem arises because the firewall node translates the View client IP address to its own before

passing the message to the SCADA server. Consequently, when two View clients try to connect, the SCADA server cannot distinguish between the two nodes because the IP addresses are equivalent.

Notes on Networking with Other iFIX and FIX Nodes

iFIX v3.5 can share data and alarms with previous versions of iFIX, as well as with FIX32 v6.15 and FIX v7.0. FIX32 view nodes will only receive alarms from alarm areas A-P.

NOTE: *You cannot run iFIX and FIX v6.x or greater at the same time on a single computer*

5. Getting Started with the SCU

This chapter helps you start configuring iFIX with the System Configuration Utility (SCU). It explains how to start and exit the SCU, complete file operations, and define the iFIX paths for your computer.

Before You Begin with the SCU

The following SCU configuration tips may help you start up and maintain your iFIX environment more efficiently.

- Configure the SCU *before* you start the Intellution iFIX WorkSpace. This way you do not have to exit the WorkSpace and restart iFIX.
- Use the local node alias feature in your computer to save development time later. Refer to the *Enabling the Local Node Alias Feature* section for more information.
- Run iFIX as a service under Windows to give you more flexibility and security in your process environment. Refer to the *Running iFIX as a Service* section for more information.
- Store your SCU files remotely on the network so that FIX Startup can access them on a file server. If you are using a file server, it may be useful to store all your SCU files in one place. In Microsoft Windows, you have another option — simply connect a networked drive to a remote server on the local network that contains the desired files or directories. This strategy increases control over configuration files and makes your routine maintenance easier.

Refer to the *iFIX Startup* chapter for detailed information regarding the startup program in iFIX.

Starting and Exiting the SCU

To properly start and configure the SCU, you should do so before you open the Intellution iFIX WorkSpace. You can start the SCU by clicking System Configuration from the iFIX program folder in your Windows Start menu. However,

if you are in the Intellution iFIX WorkSpace and you need to make changes, you can start the SCU by clicking the SCU button on the Application toolbar, or by double-clicking System Configuration in the system tree. Note that, for its first startup, the SCU uses the node name you specified during installation.

The main SCU window displays graphics and icons that represent enabled options and tools. You can click many parts of the window to bring up the related dialog box. This graphical interface lets you determine at a glance what kind of node and options the open SCU file enables. You can also disable an option by selecting the graphic or icon in the main SCU window and pressing Delete.

NOTE: *Deleting an icon from the main SCU window removes that service from your server's configuration. A dialog box appears warning you of this.*

Using the SCU Toolbox

The bottom of the SCU window contains a toolbox that includes all the tools you need to use the SCU. These tools are accessed by clicking a button in the toolbox. The table below shows what each button does.

Table 5-1: SCU Toolbox Buttons and Their Functions

Clicking the button…	**Displays the…**	**Which lets you…**
	Path Configuration dialog box.	Specify the location and names of your iFIX directories.
	Alarm Configuration dialog box.	Enable and configure alarm services.
	Network Configuration dialog box.	Configure network connections.

Table 5-1: SCU Toolbox Buttons and Their Functions (continued)

Clicking the button…	Displays the…	Which lets you…
	SCADA Configuration dialog box.	Configure SCADA servers.
	Task Configuration dialog box.	Select tasks to run automatically in various start-up modes.
	Security Configuration window.	Configure security in your process environment.
	SQL Accounts dialog box.	Create a SQL login account and configure the SQL task.
	Edit Alarm Area Database dialog box.	Edit the Alarm Area Database.

To exit the SCU, select Exit from the File menu.

SCU File Operations

The SCU file contains all of the necessary information for iFIX to run as you have specified. You can perform several operations with SCU files, as described in the following sections.

Opening a New File

When you start the SCU, it automatically opens the SCU file specified by the local startup options. If the SCU cannot find the specified file, it opens a new one. To create a new file while the SCU is open, select New from the File menu. A new SCU main window appears with no link to the process database and no drivers configured.

Adding a File Description

At the top of the SCU window, a short title appears under the menu bar. This is the name of your SCU file, also known as a file description. You can change the name so that each SCU file has a unique identifier. The file description is only there to help you distinguish between SCU files; the system does not use the description in any way.

To name your SCU file, select Description from the File menu, or double-click the title area. Enter a description of up to 40 characters in the Enter Configuration File Description field.

Creating a Report

SCU reports contain network information about your server's configuration, including the system path, and SCADA, alarm, task, and SQL configuration. To create a report of the open SCU file, select Report from the File menu, type a file name in the File name field, and click Save. The SCU notifies you whether it successfully wrote the file. You can view or print the report with any text editor or word processor.

SCU reports have an .RPT file extension and are stored in the directory pointed to by the local path.

Configuring Directory Paths

iFIX uses a number of directories to store program and data files. Use the Path Configuration dialog box to specify the location and names of your iFIX directories. You can display this dialog box by clicking the Path button on the SCU toolbox.

When iFIX is installed it creates a directory, called the Base directory, and all the subdirectories you see listed in the Path Configuration dialog box. If you decide to change the Base path, and the other directories are subdirectories of the Base path,

click Change Base to automatically update all the listed directory names. When you change a path the SCU creates the new directory for you. However, it does not copy the files from the old directory to the new directory.

NOTE: *When configuring paths for your iFIX components, it may be helpful to place some directories on the local machine and some on a network server. For example, keeping your Local and Database directories on a local path name allows you easy accessibility on your computer, whereas copying the Picture and Historical files to a network server enables anyone on the network to access these files to view a picture, historical data, and so forth.*

The table below describes the use of each directory.

Table 5-2: Path Descriptions

The path…	Is used for storing...	Default Path
Base	All executable files. The Base path points to the main iFIX directory. Other directories are usually subdirectories of the Base directory.	C:\DYNAMICS
Language	The language files used to create dialog boxes and help files. If you choose to implement a language other than English, the new language and help files replace the files found in this directory.	C:\DYNAMICS\NLS
Local	Configuration files associated with the local computer, including SCU, recipe format, and system security files.	C:\DYNAMICS\LOCAL
Project	A grouping of application files, such as pictures, databases, and tag groups, saved in a specific folder identified by the project name. You can manage your application files by naming a different path for each project.	C:\DYNAMICS

Table 5-2: Path Descriptions (continued)

The path…	Is used for storing...	Default Path
Database	Process database files, Database Builder configuration files, and I/O driver configuration files.	C:\DYNAMICS\PDB
Picture	The pictures of the configuration and run-time environments. ***NOTE:*** *If you are using a shared PIC directory on a drive other than the one on which iFIX is installed, you must enter the full path to the PIC directory. For example, if you want to use a shared PIC directory on the G:\ drive, you must enter G:\PIC in the SCU.*	C:\DYNAMICS\PIC
Application	Data and configuration files for your iFIX applications. If you create your own applications, use this directory to store data files.	C:\DYNAMICS\APP
Historical	Historical Trending configuration files.	C:\DYNAMICS\HTR
Historical Data	Historical data files. Historical Trending creates a unique subdirectory to this directory for each node that data is being collected from. The subdirectory uses the name of the node the data comes from.	C:\DYNAMICS\HTRDATA
Alarms	Alarm data files.	C:\DYNAMICS\ALM
Master Recipe	Master recipe, master recipe error, and master recipe report files.	C:\DYNAMICS\RCM

Table 5-2: Path Descriptions (continued)

The path…	Is used for storing...	Default Path
Control Recipe	Control recipe, control recipe error, and control recipe report files.	C:\DYNAMICS\RCC
Alarm Areas (AAD)	Primary Alarm Area Database files.	C:\DYNAMICS\PDB

Overview Checklist

Following is a list of general tasks for implementing the SCU in iFIX.

[1] Start the SCU before you open the Intellution iFIX WorkSpace.

[2] Configure your local startup options, including the local server name, local logical name, and the local SCU file name.

[3] Configure the path in which to store the program and data files.

[4] Make any start-up or configuration changes using the SCU toolbox and associated dialog boxes. Refer to the appropriate chapters in this manual for more information.

[5] Save any configuration changes to either a local disk or a remote file server.

6. Configuring iFIX Using the SCU

This chapter describes how to configure iFIX with the System Configuration Utility (SCU).

Configuring Local Startup Options

Local startup options allow you to define configuration options that apply only to your server. If you try to exit the SCU without specifying local startup options, the SCU warns you that iFIX will not be able to properly configure your server. Local startup options allow you to specify:

- The local server name.
- The local logical name.
- The local SCU file name.
- Whether the local server runs as a service under Windows.
- Whether the local server uses the local node alias feature.

Specifying the Local Server, Local Logical, and SCU File Name

Before you start iFIX, you need to specify the local server name, local logical name, and local SCU file name in your Windows Registry. (The Windows Registry is a database that your operating system uses to store application information.) We strongly recommend that you use the SCU to write changes to the registry for you instead of editing the registry directly.

Logical node names are used to group partner SCADA servers (primary and backup) to form a logical pair. This ensures that you can establish SCADA server failover in your SCADA network. For more information on configuring SCADA server failover using the SCU, refer to the *Advanced Topics* section. For more information on implementing SCADA server failover and LAN redundancy using iFIX, refer to the *Mastering iFIX* manual.

To choose local node, local logical, and configuration file names, select Local Startup from the Configure menu and enter the names in the appropriate fields of the Local Startup Definition dialog box. The SCU stores all SCU files created on the local server in the directory defined by the local path, unless you specify otherwise when saving the file.

NOTE: *If you enable security and set the security path to a folder other than the default, which is the Dynamics/Local folder, when you change the node name, security is disabled. You will need to configure iFIX security again and enable it.*

Running iFIX as a Service

You can run iFIX as a service under Windows. When enabled, this option allows you to close any foreground task and log out of Windows without shutting down core iFIX tasks like networking, SAC processing, alarming, and I/O driver control. This provides a much higher level of security to your process, because operators can log in and log out of a Windows server before and after their shift without affecting the process.

NOTE: *When you configure iFIX to run as a service, you should not have the WORKSPACE.EXE listed as a configured task in the Task Configuration dialog box of the SCU. Instead, you should start WorkSpace from the Startup group for the user, or have the user start WorkSpace manually. If you do not delete WORKSPACE.EXE from this list, unpredictable results may occur. For example, if you are using iHistorian, no servers appear in the Server Name field of the Configure the iHistorian Server(s) dialog box.*

There are two ways to configure iFIX to run as a service:

- Enable iFIX as a service option.
- Configure background tasks that you want to run as a service. For more information, refer to the *Configuring Startup Tasks* section.

When you run iFIX as a service, you should be aware of the following:

Windows Services

Do not shut down iFIX or make changes to the iFIX configuration from the Windows Services control panel.

Disabling iFIX as a Service

You must shut down iFIX before disabling the iFIX as a Service option in the SCU.

Starting the Intellution iFIX WorkSpace

You should not have the WORKSPACE.EXE file listed as a configured task in the Task Configuration dialog box of the SCU. Instead, you should start the Intellution iFIX WorkSpace from the Startup group for the user, or have the user start the Intellution iFIX WorkSpace manually.

iFIX Paths

Windows NT does not map network drives until a user logs in. Therefore, if running iFIX as a Service under Windows NT, all iFIX paths must be set to the local drive.

Running iFIX with Terminal Server

Running iFIX as a service under Terminal Server is not allowed.

Running iFIX with Other Programs

By default, iFIX uses the local System account when running as a service. However, you cannot use the System account with certain applications, such as the iHistorian. To configure a different user name and password for iFIX running as a service:

[1] From Control Panel:

- In Windows 2000, Windows XP, or Windows Server 2003 select Administrative Tools, then Services.
- In Windows NT, select Services.

[2] In the Services folder, right-click on Fix, then select Properties.

[3] In the Log On tab, set the user name and password for This Account to the user account you want to log in when iFIX is running as a service.

Enabling the Local Node Alias Feature

The Local Node Alias feature allows you to substitute a placeholder, THISNODE, for the node portion of a data source in order to automatically access information from the local SCADA server. This is ideal for developing pictures that can be shared among several computers that each access different SCADA servers. To use the Local Node Alias feature, you must first enable it in the Local Startup Definition dialog box.

Configuring Security

You can configure security using the Security Configuration program, which can be accessed from the SCU by clicking the Security button on the SCU toolbox.

Before starting the Security Configuration program, make sure that iFIX is running and, if security is enabled, that you have the proper account privileges.

The *Implementing Security* manual fully describes the security program.

Configuring Network Connections

You can enable network communications between any two iFIX servers by configuring each computer's network connections. To define these connections, click the Network button on the SCU toolbox.

You can use the Network Configuration dialog box to configure network protocols, configure network communications, and establish dynamic connections. Refer to the following subsections for information on all of these functions.

Configuring Protocols

iFIX allows you to establish communications with either NetBIOS or TCP/IP protocols. Configuring a protocol enables that protocol for your network.

Configuring Remote Nodes

iFIX allows you to configure primary and backup nodes for SCADA server failover. By entering a primary and backup node in the Network Configuration dialog box, you ensure connection with that node should communication with the primary node fail. The following sections describe how you can enable, configure, and modify remote nodes in your network environment.

For more information on implementing SCADA server failover in your environment, refer to the *Mastering iFIX* manual.

Enabling Backup SCADA Nodes

You must first add a remote node to your configuration before you can enable SCADA server failover in your network.

You can view or make changes to the configured remote nodes in the Remote Nodes area of the dialog box. To view the primary and backup nodes currently configured, select the Show All Names check box.

Using Network Timers on a Per-node Basis

The Remote Node Configuration dialog box allows you to modify network timer values on a per-node basis.

Refer to the *Advanced Topics* chapter for more information on configuring network timers, including what each time-out value represents.

Dynamic Connections

Dynamic connections allow iFIX to make a network connection when it needs to retrieve data from a server. For example, if a picture references a remote server, and the remote server has not been configured in the SCU, iFIX automatically makes a dynamic connection to that server when you open the picture. The servers will remain connected, even if you close the picture or exit the run-time environment. In fact, with Dynamic Connections enabled, you do not have to enter node names in the Configured Remote Nodes list at all.

When iFIX first opens a picture that requires a dynamic connection, it may take a slightly longer time resolving the connection. This delay depends on the amount of network connections required for the specific picture and if these servers are available for a connection.

The Dynamic Connections option is disabled by default, and affects all connections from the node. All dynamic connections will inherit the network timer settings defined within the SCU. If you choose to enable dynamic connections, iFIX may attempt to establish a connection when calling the System.FindObject method in a script. This happens when a name or an object is referenced in a script but is not currently loaded. For example, consider the following script:

```
Dim shape as Object
Set shape = System.FindObject("badname.rect1")
```

badname is the name of a picture that is not currently loaded. In this script, iFIX attempts to establish this connection with *badname*. When the connection fails, the following error occurs:

```
Object not found
```

NOTE: *With Dynamic Connections enabled, a new node will not receive alarms from a SCADA server until a connection is established. If you want a remote node to receive alarms from a SCADA server immediately after starting up, you should add the SCADA server name to the Configured Remote Nodes list of the View client.*

Configuring LAN Redundancy

You can configure LAN redundancy simply by enabling it in the SCU. You must have a protocol enabled so that the SCU is configured for network support.

To enable LAN redundancy, click the Advanced button on the Network Configuration dialog box. A caution message box warns you not to modify these values without familiarity with the system. If you are unsure as to how to proceed, refer to the *Advanced Topics* chapter and your network documentation. To continue, click Yes.

Refer to the *Mastering iFIX* manual for more information on configuring LAN redundancy in iFIX.

Configuring Network Timers

The Advanced Configuration dialog box allows you to change your View client's network session timer values. You can also change your network timers on a per-node basis. For more information, refer to the *Configuring Remote Nodes* section. Refer to the *Advanced Topics* chapter for more information on network session timers.

Configuring Alarms

When a process value exceeds a limit that you define, iFIX issues an alarm to inform operators of this event. You can enable and configure alarm services using the Alarm Configuration functionality of the SCU.

To configure alarms, click the Alarm button on the SCU toolbox. The following sections detail how to configure alarming functions.

Enabling Alarm Services

Alarm services give you the tools you need to customize your alarm configuration. They are flexible in that you can enable any one or all of them, and you can define settings for each service to help you implement your alarming scheme. The following alarm services are available on the Alarm Configuration dialog box:

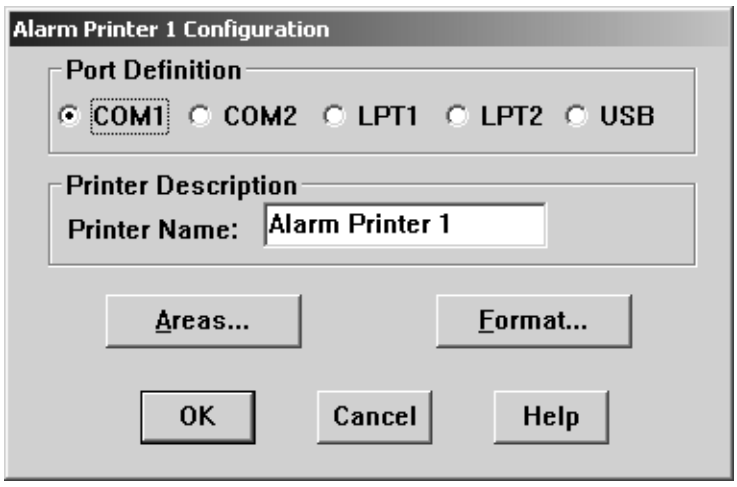
- Alarm Printers 1, 2, 3, and 4
- Alarm Summary Service
- Alarm File Service
- Alarm History Service
- Alarm Network Service (active only if you are networked)
- Alarm Startup Queue (active only if you are configured as a networked SCADA server)
- Alarm ODBC Service

To enable and configure a service, simply double-click it. For more detailed information on alarm services, refer to the *Implementing Alarms and Messages* manual. The following sections detail how you can customize alarm services using the SCU.

Customizing Alarm Services

You can modify several settings of each alarm service to customize your configuration. Each alarm service contains its own configuration dialog box with specific options that you can modify.

Refer to the *Implementing Alarms and Messages* manual for more detail on how the dialog boxes work for each service. This example shows the configuration dialog box for Alarm Printer 1.



Note that you can define many attributes to the service using one dialog box. You can also access the Alarm Areas dialog box, described in the following section.

Configuring Alarm Areas

The Configure Alarm Areas dialog box controls which alarms and application messages the alarm service can receive. You can access this dialog by clicking the Areas button on the configuration dialog box for the task you have selected.

NOTE: *You can also perform advanced alarm area configuration functions. Refer to the Advanced Alarm Configuration section for more details.*

Refer to the *Implementing Alarms and Messages* manual for more information on routing alarm areas.

The following section briefly describes how to use the Configure Alarm Areas dialog box when configuring alarm areas.

How to use the Configure Alarm Areas Dialog Box

The SCU allows you to access the Configure Alarm Areas dialog box from several locations in the interface, including the following:

Alarm Services. Double-click on an alarm service in the Alarm Configuration dialog box and then click Areas. A Configure Alarm Areas dialog box appears specific to the service you enabled.

Common Alarm Areas. Click Advanced on the Alarm Configuration dialog box and then click Common Areas. A Configured Alarm Areas dialog box appears for common areas. Note that the Use Areas Common to All Services option button is not available because you have already chosen to route to common areas.

Application Messages. Click Advanced on the Alarm Configuration dialog box and then click either Operator Messages or Recipe Messages for the messages you want to route to specified alarm areas. You can configure up to fifteen alarm areas.

There are several areas of the dialog box that help you configure your alarm areas. The following simple example illustrates how to configure alarm areas D and E to receive operator messages:

[1] **Select alarm areas**. The alarm area selection option buttons let you choose which alarm areas you want to configure.

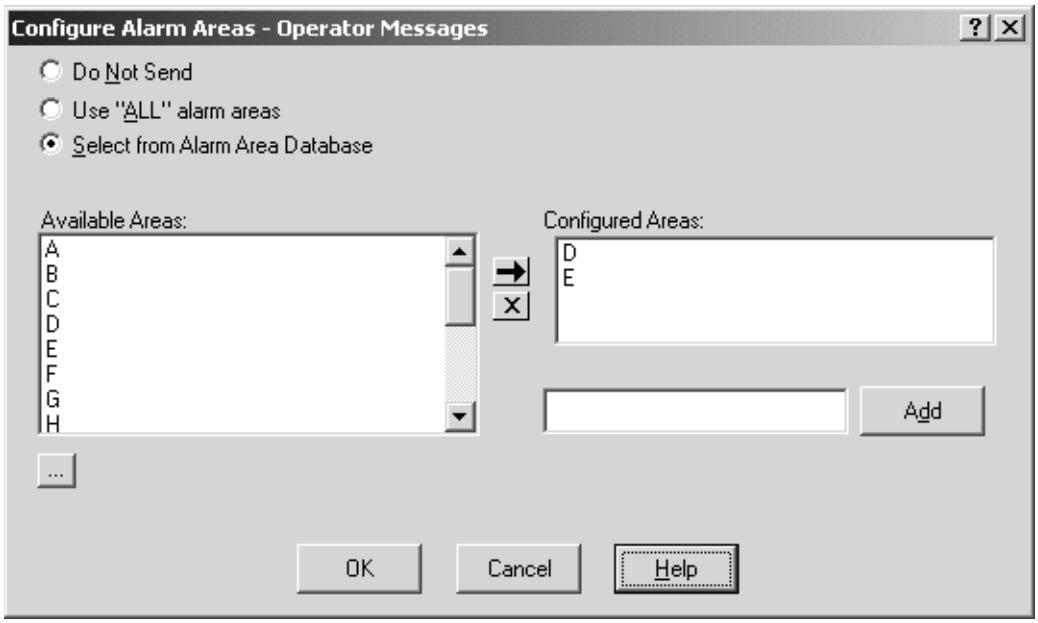
- Click the Select from Alarm Area Database option to display all areas from the alarm area database in the Available Areas list box. You can also click the Browse button to search alternate directories.

- Click the Use "ALL" Alarm areas option to add all the alarm areas in the database to the list of configured alarm areas.

- Click the Use areas common to all services option to add all the alarm areas common to all services to list of configured alarm areas.

[2] **Add alarm areas to the Configured Areas list box**. Highlight areas D and E in the Available Areas list box and click the right arrow button. This adds the selected areas to the Configured Areas list box. If you need to remove an area, highlight the area to be removed and click the X button. (If you selected Use "ALL" Alarm Areas in Step 1, the alarm area ALL is added to the Configured Areas list box. This alarm area indicates the configured alarm services receives alarms from every available alarm area.)

The following figure illustrates this procedure.



When you are finished, click OK to save your configuration, and exit the Configure Alarm Areas dialog box.

Formatting Messages

You can define the length, number of characters, and the column order for alarm or event messages. To do this, click Format on the configuration dialog box for the task you have selected, and enter the appropriate formatting options in the Message Format Configuration dialog box. This dialog box shows the column content and layout fields for block information.

To use areas common to all alarms and messages across the network, click Use Common, and configure the common messages using the Advanced Alarm Configuration dialog box. Refer to the *Advanced Alarm Configuration* section for more information.

Selecting a Port

For each printer service, you can connect the printer to serial ports (COM) 1 or 2, to parallel ports (LPT) 1 or 2, or to a USB port.

NOTE: *Printing from USB ports in Windows NT is not supported.*

Naming a Printer

The Printer Description area displays the printer that corresponds to the port selection. Rather than use a generic title, such as Alarm Printer 1, you can change the name of the printer task as it appears in the Printer Name text box.

Deleting Alarms

You can automatically or manually delete alarms using the Alarm Summary service. Select either the Automatic or Manual option buttons in the Alarm Deletion area to choose the method of alarm deletion.

Enabling the Startup Queue Configuration

Using the Startup Queue Configuration dialog box, you can configure the SCADA server to send all the alarms that have occurred prior to starting iFIX on the View client. The SCADA server sends these alarms to the iClient when the client starts. To enable the Startup Queue Configuration, double-click the Alarm Startup Queue service. The Startup Queue Configuration dialog box appears.

NOTE: *You must be configured as a SCADA server and have the Network Alarm Service enabled in order to enable the Startup Queue Service.*

By default, the Summary Alarms Only check box is selected so that the Alarm Startup Queue service delivers only the current alarms. If you want to receive additional alarms and messages, click the check box to disable this function.

NOTE: *By disabling the Summary Alarms Only option, you may receive duplicate alarms at some alarm destinations. You also increase network traffic if iClients are configured to receive alarms from the local SCADA server.*

You can also filter alarms according to a set time. To do this, select the Enable Time Filter check box and enter the hour and minute in the appropriate Filter Alarms Older Than fields.

Enabling the Alarm ODBC Service

Another valuable service you can enable in the SCU is Alarm ODBC. This service sends alarms and messages to an ODBC relational database. Once the relational database receives and stores the data, you can easily retrieve any information you want by querying the database.

For more information on the Alarm ODBC Service, refer to the *Configuring the Alarm ODBC Service* section in the *Implementing Alarms and Messages* manual.

Advanced Alarm Configuration

The SCU provides advanced functionality that gives you more ways to configure your alarm destinations. To access advanced configuration options, click the Advanced button in the Alarm Configuration dialog box.

The sections that follow summarize the functions that are available. For complete details on how to work with alarm areas, refer to the *Implementing Alarms and Messages* manual.

Configuring Common Alarm Areas

To assign alarm areas common to all services, click the Common Areas button and select the alarm areas you want.

Defining a Common Message Format

You can define a common message format for alarms and messages received by Alarm Printer, Alarm File, and Alarm History services. To do this, click the Common Format button and select or edit the properties of the messages you wish to define.

Routing Application Messages

To control which alarm areas receive application messages on other servers, configure the alarm areas for these messages. You can configure areas for either operator messages, recipe messages, or both, by clicking the Operator Messages or Recipe Messages buttons.

Modifying Alarm Queues

Sometimes a large process environment requires that you balance using system resources against handling large numbers of alarms. In order to do this, you may have to modify alarm queues so that your local SCADA server can handle the number of alarms being routed through the network. For more information on modifying alarm queues, refer to the *Implementing Alarms and Messages* manual.

Editing the Alarm Area Database

The SCU makes it easy for you to configure the Alarm Area Database. You can make changes to the database after you have configured any number of alarm areas.

To edit the alarm area database, start iFIX on the local SCADA server, click the Alarm Area Database button on the SCU toolbox. You can also access this dialog box by clicking Advanced on the Alarm Configuration dialog box and then clicking Alarm Area Database.

Using the Edit Alarm Area Database dialog box you can add, modify or delete an alarm area, or designate a name for an alarm area that is specific to your process environment. For example, you can replace the default alarm area, A, with a more intuitive name, *Main Oil Well*, by selecting A in the Configured Alarm Areas list, entering a new name in the Alarm Area field, and clicking Modify. The new name is added to the list in alphabetic order.

NOTE: *Changing alarm area names in the alarm area database automatically changes them in your process database.*

Refer to the *Implementing Alarms and Messages* manual for more information on editing the Alarm Area Database.

Configuring the Auto Alarm Manager

The Auto Alarm Manager lets you configure a remote server so that it automatically delivers alarms to a central location using the Microsoft Remote Access Service.

NOTE: *The Auto Alarm Manager only communicates over NetBIOS, and requires that Microsoft Remote Access Service (RAS) software be installed on each server running the Auto Alarm Manager. Refer to your Microsoft manuals for more information on setting up RAS.*

To access the Auto Alarm Manager feature, select Auto Alarm Manager from the Configure menu. The Auto Alarm Manager Configuration dialog box appears. Click Enable to activate all the fields. By default, the Auto Alarm Manager is disabled.

Auto Alarm Manager statistics are displayed in Mission Control so that you can easily monitor the program's progress. Refer to the *Viewing Auto Alarm Manager Statistics* section for more information.

There are several steps to configuring the Auto Alarm Manager:

[1] Specify a sending server. At minimum, you MUST specify RAS phone book entries to activate the sending server.

[2] Configure alarm filters.

[3] Specify a Windows account and password. If you configure the iFIX Startup program to run as a service of Windows on the sending server, you must also specify a Windows user account and password in the Auto Alarm Manager for use when delivering alarms.

[4] Configure your timers. To increase the efficiency of the Auto Alarm Manager's communication intervals, you can configure how long the Auto Alarm Manager has to send alarms to the receiving server, and whether to flush alarm queues upon successful or unsuccessful delivery.

[5] Specify a destination server.

Refer to the *Implementing Alarms and Messages* manual for more information on configuring the Auto Alarm Manager.

Configuring the Alarm Horn

When a new alarm occurs in the system, iFIX can notify you through the alarm horn. You can enable or disable the alarm horn from the SCU, and also from the WorkSpace through the Alarm Horn Expert. For example, you can disable the horn in SCU, then enable or disable it from the Alarm Horn Expert once iFIX has started.

It is important to note that these two alarm horn configurations work independently of each other. For example, if you disable the alarm horn in the SCU, then enable it using the alarm horn expert once iFIX has started, each time that you shutdown and restart iFIX, the horn will be disabled. This occurs because the SCU setting is the initial value and it takes effect each time that you start iFIX.

NOTE: *Shutting down and restarting the WorkSpace has no effect on the alarm horn configuration.*

For more information on running experts, refer to the *Running Experts* section in the *Creating Pictures* manual.

Configuring SCADA Servers

SCADA servers monitor process values and communicate with process hardware. To establish and configure a SCADA server, click the SCADA button on the SCU toolbox. The following subsections detail how to configure SCADA servers using the SCADA Configuration dialog box.

Enabling SCADA Support

To operate as a SCADA server, you must first enable SCADA support using the SCADA Configuration dialog box. When you enable SCADA support, the local node becomes a SCADA server capable of accessing your process hardware. You can then set up and configure I/O drivers and establish SCADA server failover in your network.

Naming the Database

Once you enable SCADA support, you can define the process database you want to load when iFIX starts. You can also change the database name from the main SCU window by double-clicking the database entry (located under the Node name entry).

NOTE: iFIX *comes with an empty database file named EMPTY.PDB. This database is read-only. By loading and saving the database to a different name you can quickly create an empty, working database. We recommend that you create a new database with a new name to prevent overwriting your work when re-installing or upgrading software.*

Configuring Drivers

iFIX provides at least one I/O driver and an optional DDE I/O driver to provide the communications link between the process hardware and iFIX. Before your SCADA server can communicate with the process hardware, you need to define and configure at least one I/O driver. iFIX can load up to eight I/O drivers during startup.

The first step in configuring your driver is to tell iFIX which driver you want to use.

Setting up the Driver

Some drivers use an interface card to communicate with the process hardware. In this case you may have to configure the interface card to use the driver.

NOTE: *Not all drivers require an interface card, so the setup field may be grayed out. Refer to your I/O driver manual for information on configuring this card.*

Configuring an I/O Driver

I/O drivers are configured using the I/O Driver Configuration program.

NOTE: *Not all drivers have a configuration program, so the Configure field may be grayed out. Also, the initial screen of the I/O Driver Configuration program varies depending on the type of driver you are configuring.*

Configuring Alarm Acknowledgement Synchronization

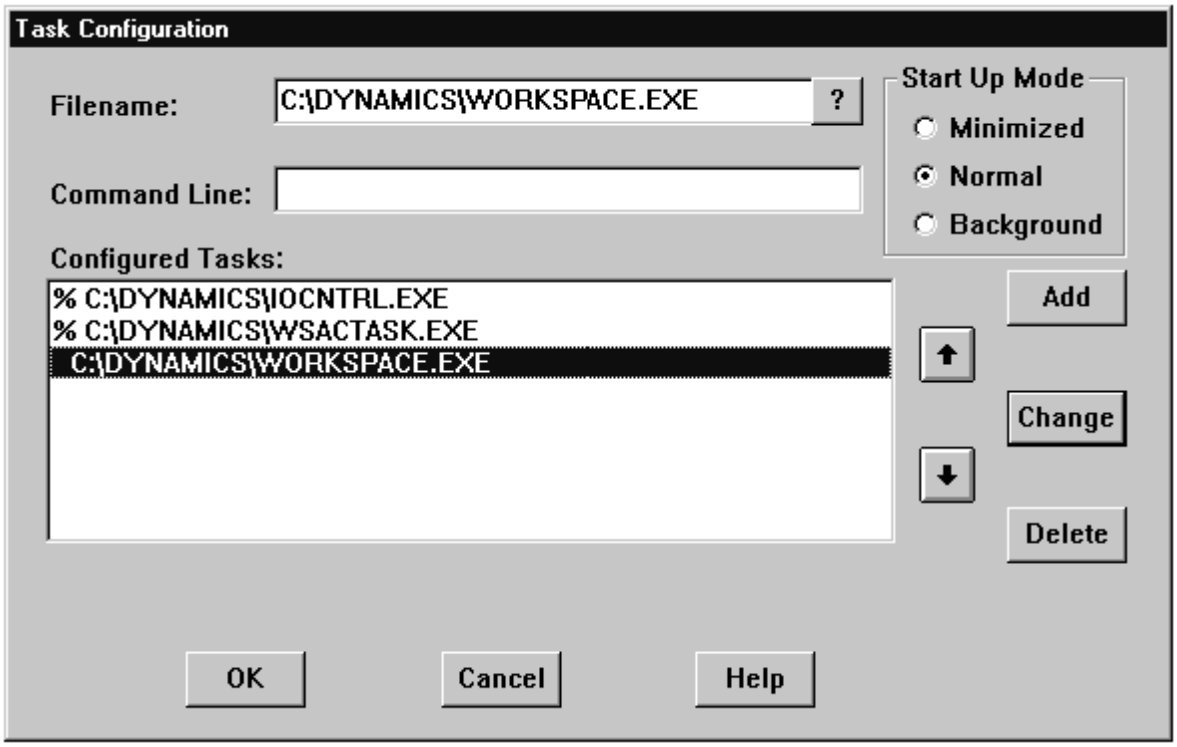
The Partner SCADA area lets you synchronize alarm acknowledgments between the local node and a remote SCADA server. You should configure alarm summary synchronization if your node is using SCADA server failover.

In a SCADA server failover configuration, when an operator acknowledges an alarm, iFIX acknowledges the alarm on both SCADA servers. If the tag re-alarms quickly after an acknowledgment, iFIX may also acknowledge the new re-issued alarm.

You can also configure SCADA server failover on your SCADA network without enabling alarm synchronization. For more information on SCADA server failover, refer to the *Failover and Redundancy* chapter in the *Mastering iFIX* manual.

Configuring Startup Tasks

You can specify tasks for automatic start-up by clicking the Task button on the SCU toolbox and displaying the Task Configuration dialog box. These tasks start when you run the FIX Startup program. For example, if you always use I/O Control when you start iFIX, configure the SCU to start IOCNTRL.EXE automatically, as depicted in the figure below.



An asterisk (*) next to a task means that Startup minimizes the task after starting it. A percent sign (%) preceding a task means that Startup starts that task in the background. To change the state of a task, select the task, select an option from the Start Up Mode area, and click Change. iFIX executes the tasks in the same order as they appear in the Configured Tasks list. To remove a task from the list, select the task from the Configured Tasks list and click Delete.

If desired, add any specific command line parameters in the Command Line field. Refer to the *Controlling SAC Startup* section for available SAC command line parameters, or refer to individual application manuals for available command line parameters for each application.

Refer to the *Running iFIX Tasks in the Background* section for information on iFIX tasks that can be started in the background.

Running iFIX Tasks in the Background

When you automatically start programs, you can specify that they run in the background so that they do not interfere with your typical operation. You should only configure the following iFIX tasks as background tasks (All of these files are located in the FIX Base path):

- SAC (WSACTASK.EXE)
- Historical Collect (HTC.EXE)
- SQL Task (WSQLODC.EXE)
- I/O Control (IOCNTRL.EXE)
- Auto Alarm Manager (AAM.EXE)
- Event Scheduler (FIXBACKGROUNDSERVER.EXE)

Controlling SAC Startup

iFIX lets you control the startup status of SAC using the task configuration of the SCU.

Starting SAC Automatically

When you enable the SCADA function, the SCU includes WSACTASK.EXE in the startup list within the Task Configuration dialog box. This starts SAC automatically.

If you disable SAC during development, you must enable it again. You can also modify how SAC operates by entering specific command line parameters. The following command line parameters are available:

- **S** — Synchronizes SAC to the system clock. Refer to the *Building a SCADA System* manual for information on scan times and synchronization.

- **Dseconds** — Delays SAC processing of the database until the I/O driver initializes and receives data from control devices. By default, SAC automatically delays processing for 8 seconds. You can use the D parameter to specify a delay of 1 to 300 seconds, for example D30, to control initial processing of database blocks.

- **Q —** Sets the number of queue entries for the Alarm Queue Status program that monitors the alarms deleted by SAC. This parameter lets you override the default (500), and prevents the queue from expanding to the maximum length of 2000.

- **C** — Suppresses communication (COMM) alarms.

  IMPORTANT: *SAC parameters do not use the slash (/) or dash (-) delimiters. Use spaces to enter optional SAC parameters.*

  ```
  For example:  S D30
  ```

Starting I/O Drivers Automatically

I/O drivers are started by the I/O Control program through the Task Configuration dialog box. When you install an I/O driver, the I/O Control program is automatically added to the list of tasks.

If you remove the I/O Control program from the task list, you can add it back again. The table below shows you the command line parameters you can use to specify how I/O drivers start.

Table 6-1: I/O Control Command Line Parameters

Parameter	Description
/A	Starts all I/O drivers identified in the SCADA configuration.
/S*xxx*	Starts one I/O driver, where *xxx* is the three letter I/O driver acronym. For example, /SABH.
/D*xxx*	Delays the startup of a driver where *xxx* is the delay time in seconds.
/AP*xxx*	Sets the message rate for all drivers, where *xxx* is a value of 1 to 100.
/SdrvP*xxx*	Sets a specific driver's message rate, where *xxx* is a value of 1 to 100.

NOTE: *FIX I/O drivers v7.x or greater automatically start communicating with their OPC server. No command line parameter is needed.*

Configuring iFIX for Relational Databases

iFIX supports many relational databases, such as Oracle®, Sybase, and Microsoft® SQL Server through Microsoft's industry-standard Open Database Connectivity (ODBC). Using the SCU, you can set up your server to access multiple relational databases from a process database. The SCU's SQL functionality allows you to read and write data between a SCADA server's process database and multiple relational databases.

To access a relational database data source, you must first do the following:

[1] Set up your relational database and ODBC driver.

[2] Configure the ODBC data source.

[3] Add the database to the SQL connection list.

[4] Create the library and error tables.

For more information on accessing relational database data sources, refer to the *Installing and Configuring Data Sources* chapter in the *Using SQL* manual.

Configuring the SQL Service

The SQL Task Configuration dialog box lets you configure the SQL service, including enabling SQL support, specifying a backup file location, identifying a relational database, routing SQL errors and messages to alarm areas, and defining a sleep interval.

For more information on configuring the SQL service, refer to the *Configuring the SQL Task* chapter in the *Using SQL* manual.

7. Using the Startup Profile Manager

The Startup Profile Manager is a utility that allows you to link users to projects or configurations, as well as restrict the actions that these users can take when starting iFIX. With the Startup Profile Manager, you create unique startup profiles for individual iFIX users, as well as a default profile for all other users.

The following figure shows an example of the main window of the Startup Profile Manager that appears when you open the application.

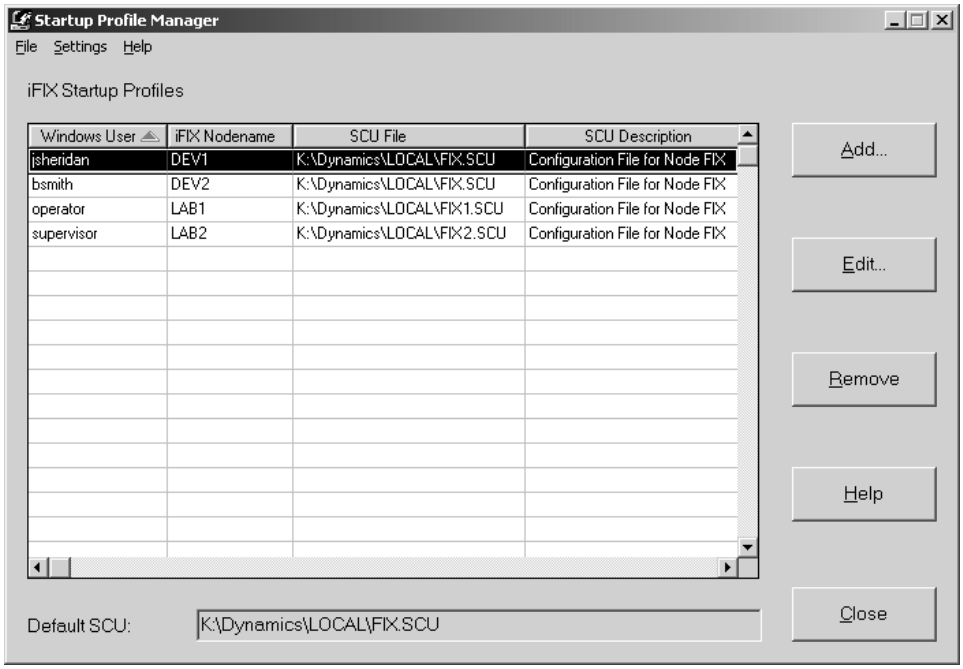


Figure 7-1: Startup Profile Manager

What Exactly is a Startup Profile?

A startup profile is a group of settings that associate a Windows user name with a specific iFIX Project Configuration. The iFIX Project Configuration includes:

- SCU path and file name that you want the specified Windows user to use when starting iFIX.
- Node name that you want the specified Windows user to use when starting iFIX.
- Restrictions on whether the user can modify these settings during iFIX startup.
- Restriction on whether the user can run the iFIX Sample System.

When starting, iFIX checks the currently logged in Windows user name to determine if the user has a profile listed in the Startup Profile Manager. If a profile is identified, iFIX loads that profile. Otherwise, the default profile is used, if it is enabled. If a default profile does not exist, no profiles are loaded. In this case, iFIX loads the node and SCU file defined in the Local Startup Definition dialog box of the SCU application (which is the SCU file and node name defined in the Windows Registry), and there are no restrictions in the iFIX Startup dialog box, unless you changed the default iFIX Startup options in the Default Startup Profile dialog box of the Startup Profile Manager.

When Would You Use the Startup Profile Manager?

Use the Startup Profile Manager when you need to manage many iFIX users, such as when you use Terminal Services. For instance, with the Startup Profile Manager, you can globally define a default profile for all Windows users without profiles, and then create specific profiles for specific Windows users. Management of many user profiles is easily performed at a global level and an individual user level.

In the first iFIX release that included support for Terminal Services, iFIX v2.5, iFIX required that you generate a complete application environment for each remote user. For example, if there are 50 iFIX users, there must be 50 sets of SCU files, with each

SCU file unique to that specific user. With the Startup Profile Manager for iFIX v3.5, all user profiles are stored in a master list, making it easy to maintain and modify profiles for use with Terminal Services.

If you are upgrading from a previous iFIX release, the use of a default profile will help you in migrating from the multiple SCU files to the easier configuration in the Startup Profile Manager.

For more details on best practices when configuring Terminal Services with the Startup Profile Manager, refer to the *Using Terminal Server* manual.

Understanding Startup Profiles When Upgrading from a Previous iFIX Release

If you do not create startup profiles for your users, your existing startup configurations from previous iFIX releases run unchanged. If you later choose to create new startup profiles, the Startup Profile Manager includes an option that allows the new profile settings to override the pre-existing configurations. For more information on the override setting, refer to the *Configuring the Options for the Startup Profile Manager* section.

Startup Profile Manager Basics

There is certain basic information you should know before using the Startup Profile Manager. This section contains information on the following:

- *Configuring the Options for the Startup Profile Manager*
- *Configuring the Default Profile*
- *Security Considerations when Using the Startup Profile Manager*
- *Key Combinations Available in the Startup Profile Manager*
- *Working with Startup Profiles*

Configuring the Options for the Startup Profile Manager

Before you begin working with the Startup Profile Manager, you should configure the options that you want the Startup Profile Manager to use. *Figure 7-2* shows the Options dialog box that appears in the Startup Profile Manager.

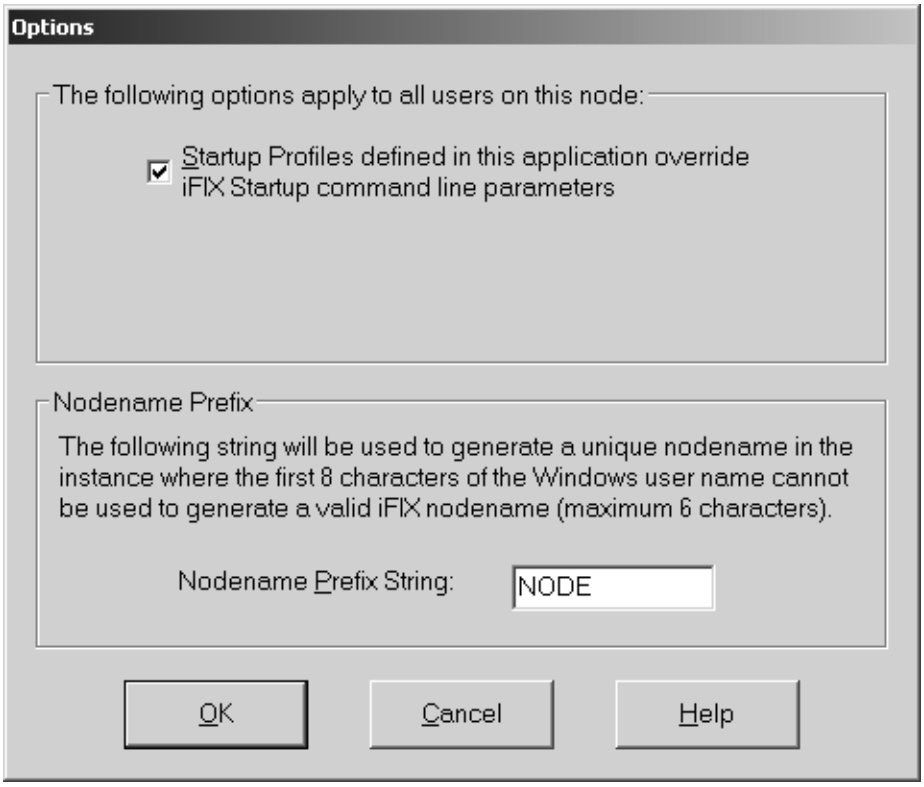

Options
The following options apply to all users on this node:
Startup Profiles defined in this application override iFIX Startup command line parameters
Nodename Prefix
The following string will be used to generate a unique nodename in the instance where the first 8 characters of the Windows user name cannot be used to generate a valid iFIX nodename (maximum 6 characters).
Nodename Prefix String:
NODE
OK
Cancel
Help

Figure 7-2: Options Dialog Box in Startup Profile Manager

To change the options for the Startup Profile Manager:

[1] Select Options from the Settings menu. The Options dialog box appears.

[2] Select the *Startup Profiles defined in this application override iFIX Startup command line parameters* check box, if you want the profiles created in this application to override the ones used when you start iFIX from the command line.

IMPORTANT: *For the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled. This override only applies to the /n, /s, and /l command line options.*

[3] Enter a string for the default iFIX node name prefix to use if the first 8 characters of the Windows user name cannot be used to generate a valid iFIX node name.

The Windows user name is an invalid iFIX node name, for instance, when the name starts with a number. Valid node names can be up to eight characters long. Node names can include alphanumeric characters, but must begin with a letter. Special characters, such as symbols and punctuation marks, cannot be used.

For each startup profile using the default iFIX node name, a number is also added to the end of the default node name, starting with the number 1. For example, if you enter NODE as the prefix, the default iFIX node names used are: NODE1, NODE2, NODE3, and so on. Each default user who starts iFIX receives a different node name.

[4] Click OK.

Configuring the Default Profile

After configuring the application options for the Startup Profile Manager, you should define a default profile, if your iFIX configuration requires it. For instance, when using Terminal Services with the Startup Profile Manager, you will most likely want to configure a default profile.

If a user attempts to start iFIX and a profile does not exist for that user yet, iFIX starts with the default profile information.

To configure the SCU and iFIX Startup options for the default profile, use the Default Startup Profile dialog box, as shown in *Figure 7-3*.

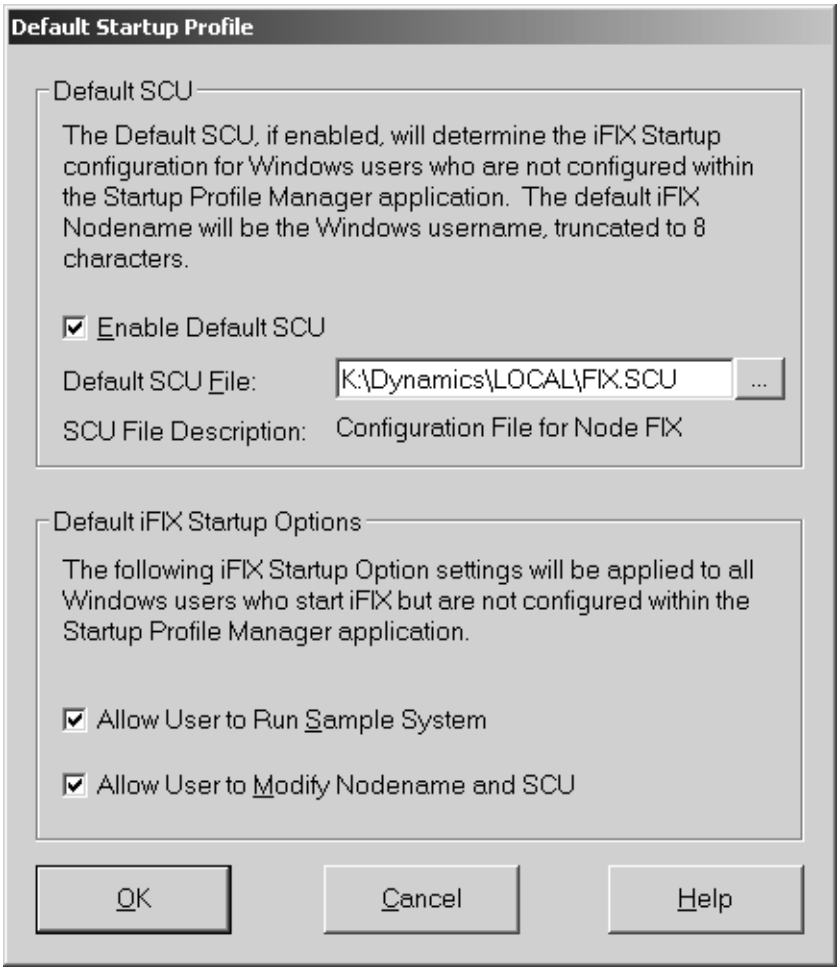

Default Startup Profile
Default SCU
The Default SCU, if enabled, will determine the iFIX Startup configuration for Windows users who are not configured within the Startup Profile Manager application. The default iFIX Nodename will be the Windows username, truncated to 8 characters.
Enable Default SCU
Default SCU File:
K:\Dynamics\LOCAL\FIX.SCU
...
SCU File Description:
Configuration File for Node FIX
Default iFIX Startup Options
The following iFIX Startup Option settings will be applied to all Windows users who start iFIX but are not configured within the Startup Profile Manager application.
Allow User to Run Sample System
Allow User to Modify Nodename and SCU
OK
Cancel
Help

Figure 7-3: Default Startup Profile Dialog Box

Security Considerations when Using the Startup Profile Manager

If you select the Enable the Default SCU option in the Startup Profile Manager, make sure you also enable the global security paths (Use These Paths for All Startup Profiles) option in the Configuration dialog box in the Security Configuration application. When you enable the global security paths, all iFIX user sessions on a computer share the same security configuration.

If you do not enable global security paths, you will need to individually configure security within each Terminal Services user session.

For more information on global security paths, refer to *Configuring Global Security Paths* in the *Implementing Security* manual.

For information on how to enable the default startup profile, refer to the *Configuring the Default Profile* section.

Key Combinations Available in the Startup Profile Manager

The following list summarizes the quick keys that you can enter from the keyboard and the actions that they perform.

Table 7-1: Startup Profile Manager Key Combinations

Enter this Key Combination...	**To...**
Ctrl+D	Open the Default Startup Profile dialog box.
Ctrl+O	Open the Options dialog box.
Ctrl+A	Open the Add Startup Profile dialog box.
Ctrl+S	Save the current startup profiles that you created.

Working with Startup Profiles

iFIX must be running in order to use the Startup Profile Manager application. After you create your startup profiles and configure the default profile (if required), you need to save your startup profiles if you want iFIX to use them. If you do not save your startup profiles during the current session, a message box reminds you to save when you exit the Startup Profile Manager.

A startup profile is not used by iFIX until the specified user attempts to start iFIX from the iFIX Startup dialog box or from the iFIX Startup command line (from a desktop shortcut or the Run dialog box, for example). If no iFIX startup profile exists

for the user and you do not define any settings in the Default User Profile dialog box or provide command line settings to the iFIX Startup application, when you restart iFIX, it displays the information from the last time iFIX was run.

General Overview of Steps for Using the Startup Profile Manager

This section outlines the general steps for getting started with the Startup Profile Manager. To begin working with the Startup Profile Manager, follow these steps:

[1] Configure the default profile in the Startup Profile Manager, if required.

[2] Configure global security paths in the Security Configuration application, if you enable the default profile.

[3] Add startup profiles in the Startup Profile Manager.

[4] Save your profiles.

Disabling or Hiding Options in the iFIX Startup Dialog Box

Using the Startup Profile Manager you can disable buttons or text edit fields that appear in the iFIX Startup dialog box on a per-user basis. To do this, you must edit the iFIX Startup Options for the user's profile. To cover users that do not have startup profiles, you should edit the Default iFIX Startup Options in the Default Startup Profile dialog box.

The following table describes the options that you disable or hide in the iFIX Startup dialog box.

Table 7-1: Disabling or Hiding Options in the iFIX Startup Dialog Box

To Disable or Hide the...	Clear this check box...
Node Name and SCU text edit fields, as well as the SCU button	Allow User to Modify Nodename and SCU
Sample System button	Allow User to Run Sample System
Entire iFIX Startup dialog box with startup options	Allow User to Run Sample System and the Allow User to Modify Nodename

For more information on the iFIX Startup dialog box, refer to *iFIX Startup* section in the *Setting up the Environment* manual.

Frequently Asked Questions About the Startup Profile Manager

The following list outlines some of the frequently asked questions about using the Startup Profile Manager.

When Does iFIX Use the Startup Profiles That You Create?

iFIX does not use the startup profiles that you create and modify in the Startup Profile Manager application until a profiled user attempts to start iFIX. When starting, iFIX checks the currently logged in Windows user name to determine if the user has a profile listed in the Startup Profile Manager.

The Override iFIX Startup Command Line Parameters Option in the Startup Profile Manager Does Not Appear to Work... Why?

The check box in the Startup Profile Manager to override the iFIX startup command line parameters (the *Startup Profiles defined in this application override iFIX Startup command line parameters* option in the Options dialog box) only applies to the /n, /s,

and /l command line options. In addition, for the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled.

How Do I Override the /e Command Line Option?

The only way to override the /e command line option (to shut down the currently running iFIX application) is to clear the Allow User to Run Sample System check box for the specified user's startup profile or, if the user is not defined, for the default profile in the Startup Profile Manager.

How Do I Stop the iFIX Startup Dialog Box From Appearing?

If you clear both the Allow User to Run Sample System and the Allow User to Modify Nodename check boxes for the iFIX Startup Options in the Startup Profile Manager, the iFIX Startup dialog box does not appear for the specified user.

If I am Upgrading from a Previous Release, Do I Have to Use Startup Profiles?

No. Your existing startup configurations will run without changes. If you later choose to create new startup profiles, the Startup Profile Manager includes an option that allows the new profile settings that you create to override the pre-existing configurations. For more information on the override setting, refer to the *Configuring the Options for the Startup Profile Manager* section.

8. iFIX Startup

The iFIX Startup program reads the SCU file and runs the tasks that support your configuration. Except for the SCU, individual iFIX applications cannot be run unless you start iFIX.

Before you start iFIX, you must make sure that you have set up the hardware, software, and network components necessary to operate iFIX in your process environment. Refer to the appropriate chapters in this manual to help you configure your environment.

When you start iFIX, the iFIX Startup dialog box appears, if you configured it to do so. From this dialog box, you can launch the iFIX Sample System, or change the iFIX node or SCU file used when iFIX starts, if you have privileges to do so. The *Figure 8-1* shows an example of the iFIX Startup dialog box with all options enabled.

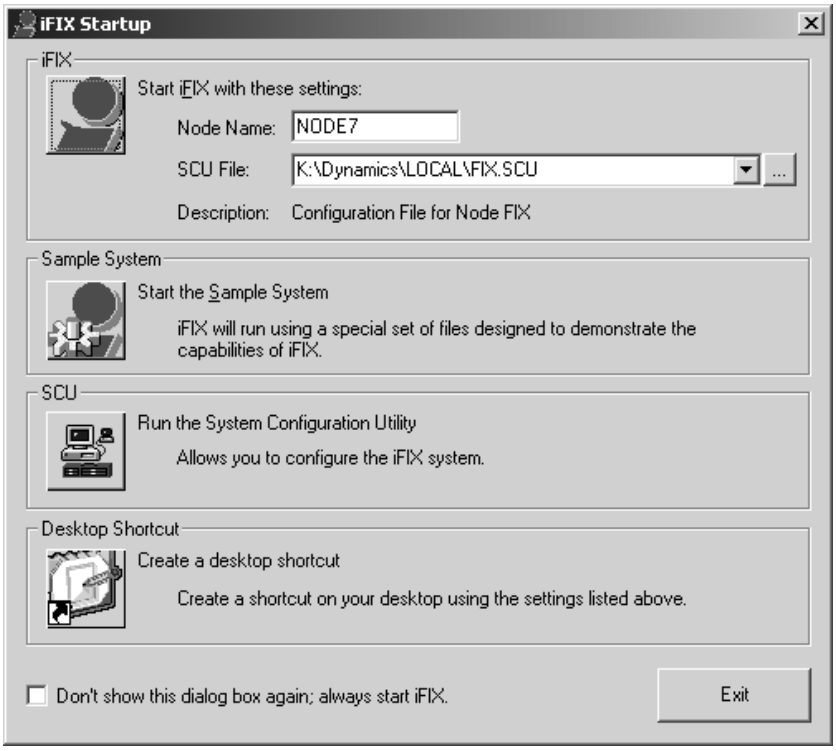

iFIX Startup
iFIX
Start iFIX with these settings:
Node Name:
NODE7
SCU File:
K:\Dynamics\LOCAL\FIX.SCU
...
Description:
Configuration File for Node FIX
Sample System
Start the Sample System
iFIX will run using a special set of files designed to demonstrate the capabilities of iFIX.
SCU
Run the System Configuration Utility
Allows you to configure the iFIX system.
Desktop Shortcut
Create a desktop shortcut
Create a shortcut on your desktop using the settings listed above.
Don't show this dialog box again; always start iFIX.
Exit

Figure 8-1: iFIX Startup Dialog Box

The privileges for your startup profile are defined in the Startup Profile Manager. For more information on how to configure startup options in the Startup Profile Manager, refer to the *Using the Startup Profile Manager* chapter in this manual. If you do not use the Startup Profile Manager, iFIX starts with the node name and SCU file last specified in the SCU.

Once iFIX loads, a dialog box appears with a message such as: "iFIX Software is currently running!" or "iFIX Demo System is currently running!"

Running iFIX From the Command Line

You can run iFIX from the command line with the Launch.exe command. Launch.exe resides in your iFIX base path. The following table describes the command line options available for the Launch.exe program.

Table 8-1: Launch Command Line Options

Option	Description
/s *SCUfile*	Starts iFIX with the specified SCU file, if you have privileges to change the SCU. This option prevents the Startup dialog box from displaying, unless the /g is also on the command line.
/n *NodeName*	Starts iFIX with the specified node name, if you have privileges to change the node name. This option prevents the Startup dialog box from displaying, unless the /g is also on the command line.
/r	Restarts iFIX, if you have privileges to do so. If the iFIX Startup dialog box displays, continue by clicking the start iFIX button. If there are other command line options that prevent the Startup dialog box from displaying, then it is prevented and iFIX automatically restarts.
/l *LogicalNodeName*	Starts iFIX with the specified logical node name.

Table 8-1: Launch Command Line Options

Option	Description
/e	Shuts down the currently running iFIX application, if the user has privileges to do so. iFIX does not display the iFIX Startup dialog box, nor does it try to restart iFIX. All other command line options are ignored. ***NOTE:*** *The only way to override the /e command line option is to clear the Allow User to Run Sample System check box for the specified user's startup profile or, if the user is not defined, for the default profile in the Startup Profile Manager.*
/t	Starts iFIX in Demo mode.
/g	Always displays the iFIX Startup dialog box, if the user has the privileges to do so. This option overrides the Don't Show This Dialog Box Again check box settings in the iFIX Startup dialog box.
/d	Automatically starts the iFIX Sample System. Prevents the Startup dialog box from displaying, unless you include the /g option on the command line.
/w *NumSeconds*	Indicates the maximum amount of time that iFIX waits for a Terminal Server session to start. If the Terminal Server session does not start, the connection times out.

NOTE: *The check box in the Startup Profile Manager to override the iFIX startup command line parameters (the* Startup Profiles defined in this application override iFIX Startup command line parameters *option in the Options dialog box) only applies to the /n, /s, and /l command line options. In addition, for the override to work, the user must be defined in the Startup Profile Manager, or if the user is not defined, the default profile must be enabled. For more information on the Startup Profile Manager, refer to the Using the Startup Profile Manager chapter in this manual.*

iFIX Startup Options

Once iFIX starts, the Startup dialog box displays a message and the Options menu is available from this dialog box. For example, *Figure 8-2* shows the iFIX Startup dialog box after you start iFIX in demo mode. Notice the Options menu on the left-hand side of the dialog box and the message, “iFIX Demo System Running!” that appears under the menu bar.

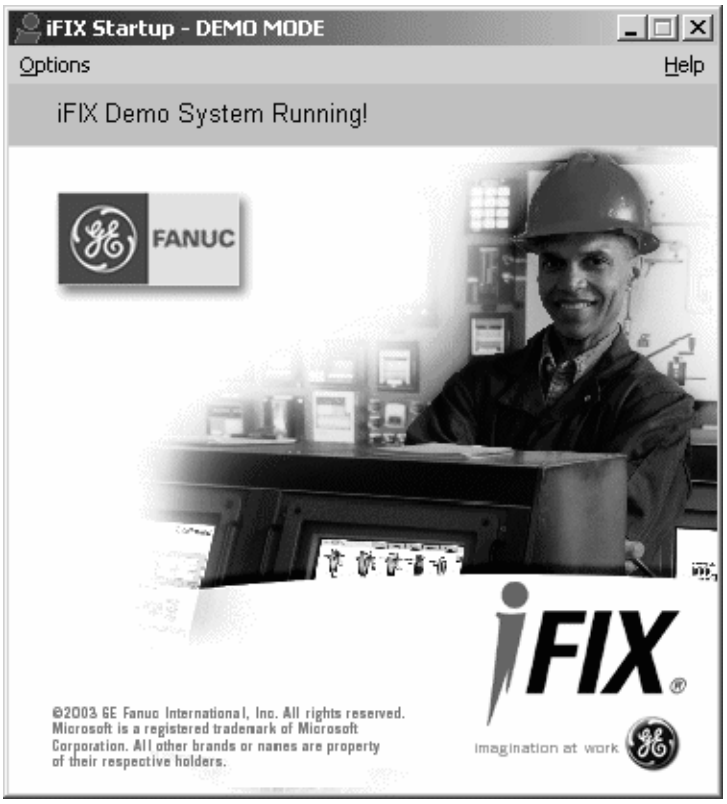


Figure 8-2: iFIX Startup Dialog Box with Options Menu

The Options menu on the iFIX Startup window lets you define startup window properties and view general conditions. These conditions are outlined in the following sections:

- *Minimize After Startup*
- *Show History*
- *Registered Tasks*
- *Shutdown*

Minimize After Startup

By default, the iFIX Startup window minimizes on your screen after iFIX loads the startup tasks. To choose not to minimize the window at future startups, deselect Minimize after Startup from the Options menu.

Show History

To view a history of startup messages, select Show History from the Options menu. The Startup History dialog box appears.

Registered Tasks

To see a list of iFIX tasks currently running on this node, select Registered Tasks from the Options menu. The Task List dialog box appears.

Shutdown

To exit iFIX select Shutdown iFIX from the Options menu. iFIX automatically closes any remaining open tasks before shutting itself down. If you have any open files, you are prompted to save changes before exiting.

To determine what version of iFIX you are running, select About from the Help menu.

iFIX Background Tasks

iFIX starts and stops background tasks based on the configuration information in the SCU file. The table below describes the function of each iFIX background task. *Automatic* tasks are started by iFIX if required by your configuration. Tasks listed as *optional* require that you start them manually by adding them to the configured task list in the Task Configuration dialog box in the SCU.

NOTE: *If you want, you can configure certain tasks to start up automatically. Refer to the Configuring Startup Tasks section for more information.*

Table 8-2: System Tasks

Program	Executable File	Function
Alarm File Task (Automatic)	ALMFILE.EXE	Receives alarm messages and stores them in files.
Alarm Printer Task (Automatic)	ALMPRIN.EXE	Receives alarm messages and sends them to printers.
Alarm Summary Task (Automatic)	ALMSUM.EXE	Receives alarms for display in the Intellution WorkSpace through the Alarm Summary object.
Alarm Manager (Automatic)	NAM.EXE	Distributes alarm messages over the network. Alarm managers run on SCADA servers.
Alarm Client (Automatic)	NAC.EXE	Receives alarm messages over the network.
Historical Collect (Optional)	HTC.EXE	Collects data according to the Historical Assign configuration file.
I/O Control (Automatic, SCADA)	IOCNTRL.EXE	Starts the I/O drivers, and displays the status of the installed I/O drivers running on the SCADA server.

Table 8-2: System Tasks (continued)

Program	Executable File	Function
Summary Queue Delete (Automatic, SCADA)	SUMQDEL.EXE	Removes the acknowledged, returned to normal, alarms from the Alarm Summary queue.
Scan Alarm and Control (Automatic, SCADA)	WSACTASK.EXE	Updates the database with data from the I/O driver, makes requested writes to the I/O Driver, generates alarms, and executes the logic of the database chains.
Network Diagnostics (Optional)	NETDIAG.EXE	Displays the status of sessions on the local node.
TCP/IP Task (Automatic)	TCPTASK.EXE	Supports node-to-node communication over TCP/IP.
NetBIOS Task (Automatic)	NBTASK.EXE	Supports node-to-node communication over NetBIOS.
Node Name Table (Automatic)	NNTABLE.EXE	Stores network information about the local and remote nodes.
Connection Manager (Automatic)	CONMGR.EXE	During startup, establishes the sessions listed in the configuration file. Monitors the status of sessions on the local node and generates alarm messages if sessions go down. It also attempts to re-establish sessions that have gone down.
Alarm ODBC Service (Automatic)	AlmODBC.EXE	Reads alarms and messages generated by iFIX and logs them to an ODBC-compliant database.

Table 8-2: System Tasks (continued)

Program	Executable File	Function
Event Scheduler (Optional)	FixBackgroundServer.EXE	Runs time and event-based scripts, allowing you to schedule reports and monitor events.
Workspace (Optional)	Workspace.EXE	Opens the iFIX WorkSpace where you can open or edit or view (in run mode) an iFIX document.

9. Monitoring the Environment with Mission Control

Mission Control provides an easy-to-use interface for monitoring iFIX programs that run in the background. It provides you with a *window* into your system, helping you diagnose potential problems with your iFIX system, and helping you improve performance on your server.

Mission Control monitors the following iFIX background tasks:

- I/O Control
- Historical Collect
- SQL task
- SAC processing
- Auto Alarm Manager
- Alarm Synchronization
- Alarm ODBC services

NOTE: *To run a* iFIX *task in the background you need to configure the program's startup task configuration in the SCU. For more information, refer to the Configuring Startup Tasks section.*

To start Mission Control, click the Mission Control button on the Application toolbar, or select Mission Control from the Intellution WorkSpace system tree. To access a particular background task, select its tab.

Each tabbed page is summarized below:

I/O Control — allows you to monitor I/O driver communications statistics and errors. For a description of these fields, refer to your I/O driver manual.

HTC — allows you to start and stop the Historical Collect background task, and provides you with an Overrun Counter. The Overrun counter increments by one every time a historical collection fails. By examining the number of HTC overruns, you can find out if there is a problem in your collection scheme. See the *Trending Historical Data* manual for more information.

SQL — allows you to start and stop the SQL task, and also provides information to help you monitor your SQL connections to ODBC relational databases. For more information on the SQL task, see the *Using SQL* manual.

SAC — allows you to start and stop the SAC (Scan, Alarm, and Control) task, and also provides SAC statistics that may help you troubleshoot your system. For example, the Blocks/Sec field can be used to monitor the amount of blocks that are scanned per second. If the number fluctuates drastically, the blocks in your iFIX database may not be properly phased. See the *Building a SCADA System* manual for more information on SAC and phasing.

AAM — allows you to monitor the Auto Alarm Manager during setup and operation, and lets you view messages pertinent to its operation. For more information, refer to the *Configuring the Auto Alarm Manager* section. Also refer to the *Troubleshooting* chapter for common messages displayed in Mission Control and their meaning.

Alarm Synchronization — allows you to monitor alarm acknowledgments synchronized by iFIX. Alarm acknowledgement synchronization is activated by specifying a partner SCADA in the SCU, and the statistics monitor sequential activity from the alarm acknowledgement synchronization task. As alarm packets are presented to the task and alarms are subsequently processed, any error statistics are displayed in the Alarm Synchronization fields from top to bottom. For more information on alarm acknowledgement synchronization, refer to the *Mastering iFIX* manual.

Alarm ODBC — allows you to send alarms and messages to an ODBC relational database. Once the relational database receives and stores the data, you can easily retrieve any information you want by querying the database. For more information on the Alarm ODBC Service, refer to the *Configuring the Alarm ODBC Service* section of the *Implementing Alarms and Messages* manual.

To close Mission Control, click the Close button at the bottom of the dialog box.

NOTE: *Closing Mission Control does not terminate the tasks that it monitors; it only closes the dialog box itself.*

Starting I/O Drivers Manually

Even if you have configured an I/O driver to automatically start, you may still want to manually start or stop the I/O driver. For example, when troubleshooting, you may need to stop the driver temporarily and then restart it.

To start I/O drivers manually in Mission Control, click the I/O Control tab. You can select a driver name from the Drivers list box. To start the selected driver, click Start. To stop the driver, click Stop.

For a description of the fields on the I/O Control tabbed page, refer to the *I/O Control Tabbed Page Fields* section.

Tuning the Driver's Message Rate

You can set an I/O driver's message rate to fine-tine your driver's configuration. To do this, click the Period button and enter a driver period. Follow these guidelines for setting the driver period:

- Enter a value from 1 through 100 in the field. The timer cycle ranges from 1/100 to 100/100 of a second. The default is 5.
- Enter 1 to get the fastest message time (100 messages per second).
- Enter 5 to get a slower message time (20 messages per second).

The driver period can also be specified in the Command Line of the Task Configuration dialog box. Refer to the *Configuring Startup Tasks* section for more information.

CAUTION: *Speeding up the message rate can adversely affect the overall performance of your system, including SAC.*

The Datascope Program

The Datascope program displays data that the I/O driver is reading. Refer to your specific I/O driver manual, as well as your process hardware manuals, for more information on the data shown on the Datascope screen.

Starting and Stopping Historical Collect

To start Historical Collect (HTC), click Start. To stop HTC, click Stop. The HTC tabbed page also displays the number of overruns that have occurred while collecting data. For more information on how HTC works, refer to the *Trending Historical Data* manual.

Viewing SQL Statistics

Mission Control allows you to view SQL statistics while you are connected to an ODBC-supported relational database. Click Start on the SQL tabbed page to load and display SQL data. The statistics displayed correspond to the SQL account and database information you have configured in the SCU. The buttons on the bottom of the tabbed page let you view specific configuration information relating to your ODBC connection. For a description of the fields on the SQL tabbed page, refer to the *SQL Tabbed Page Fields* section.

Refer to the *Configuring iFIX for Relational Databases* section for more information on SQL setup. For additional information on SQL, refer to the *Using SQL* manual.

Viewing SAC Information

You can use the SAC tabbed page of Mission Control to display real-time information on SAC performance.

For more information on SAC, refer to the *Scan, Alarm, and Control Program* section of the *Understanding iFIX* manual.

Viewing Auto Alarm Manager Statistics

Using the AAM tabbed page in Mission Control, you can view run-time messages and troubleshooting statistics in a scrollable window.

The lower portion of the tabbed page contains fields that the Auto Alarm Manager uses to display alarm statistics. As alarms are received from the user queue, the number of the alarms is displayed, and errors relating to the alarms are displayed in

the remaining fields from top to bottom. These statistics can help you troubleshoot the sending and receiving of alarms. To reset the displayed values, click Reset Statistics.

For a description of the fields on the AAM tabbed page, refer to the *Auto Alarm Manager Tabbed Page Fields* section.

Refer to the *Troubleshooting* chapter for an explanation of the messages that are displayed in the Auto Alarm Manager. Refer to the *Implementing Alarms and Messages* manual for more information on how the Auto Alarm Manager works.

Viewing Alarm Acknowledgement Synchronization Statistics

When you configure your SCADA server in the SCU, you have the option to specify a partner SCADA. This option allows you to configure a backup SCADA that is used to synchronize alarm acknowledgments. You can monitor these acknowledgments in Mission Control using the Alarm Synchronization tabbed page.

Statistics are displayed sequentially based on when the alarm acknowledgement synchronization task processes an alarm. As alarm packets are presented to the alarm task and then processed by the task, the number of packets and processed alarms are displayed. Error information relating to the processed alarms is displayed in the fields from top to bottom. To reset the displayed values, click Reset Statistics.

For a description of the fields on the Alarm Synchronization tabbed page, refer to the *Alarm Synchronization Tabbed Page Fields* section.

Viewing Alarm ODBC Information

When enabled in the SCU, the Alarm ODBC service sends alarms and messages to an ODBC relational database. The Alarm ODBC tabbed page allows you to view these alarms and messages by querying the statistics using pre-defined fields.

To save and apply the performance tuning parameters to the local path, click Save. To change the logging state, click Pause.

For a description of the fields on the Alarm ODBC tabbed page, refer to the *Alarm ODBC Tabbed Page Fields* section.

For more information on the Alarm ODBC service, refer to the *Configuring the Alarm ODBC Service* section in the *Implementing Alarms and Messages* manual.

10. Advanced Topics

This chapter provides you with additional information you can use to configure and tune the network for iFIX. The chapter also describes how you can set up partner SCADA server failover in the SCU.

Understanding Network Load

You should consider optimizing iFIX to reduce network traffic when your network configuration contains slow links. Slow links are communication links with speeds between 2400bps to 128Kbps. In networks where the slowest link is greater than 256Kbps, the iFIX network load is generally low enough that it does not need to be optimized.

Understanding network messaging is important when planning for network load over a wide area network or other network configurations that contain slow links. To understand network messaging, let's review iFIX architecture.

iFIX uses a client-server model for peer-to-peer communication to share data and alarms in real-time between nodes on a network. For data access, you can consider a iClient node to be a client and a SCADA node to be a server.

All iFIX network conversations are based on transactions. The iClient sends a request to a SCADA server. After the SCADA server acts on the request, it sends a response to the iClient. Network messages are either requests or responses.

The maximum length for a message sent by iFIX to the network interface is 16 kilobytes. One 16 kilobyte message sent by iFIX may be represented on the wire by multiple network packets. The network transport itself also sends network packets for managing the communications between the two nodes and to ensure network messages arrive without errors.

Understanding Network Sessions

All iFIX network traffic is session-oriented. Transactions between two nodes occur over a session. Before a View client can initiate a request, a session must be established with the SCADA server.

NetBIOS sessions are one-way, that is transactions can only be started by the iClient. In order for transactions to occur in the opposite direction, a second session must be established between the two computers.

Two sessions are established when using iFIX on a NetBIOS network. Only one socket is created when using iFIX on a TCP/IP network. However, two logical sessions are maintained. The session initiated by the iClient is used to retrieve data from the SCADA servers. Another session is established from a SCADA server to an iClient to send alarms to the client. In this case, the request portion of the transaction consists of the alarm data and is acknowledged by a response. These two logical sessions are maintained over one physical connection.

To establish a connection, the address of the remote node must be obtained. The method of finding this address, address resolution, is especially important for Wide Area Network (WAN) environments. NetBIOS typically uses broadcast requests to find the address of a remote node. These broadcasts can continue frequently if the remote node does not respond. This can be very disruptive over a WAN. Intellution recommends using iFIX TCP/IP networking for WAN environments. This configuration resolves the broadcast request issue.

Understanding Data Transfer

iFIX applications retrieve real-time data from an OPC server through requests. The most important iFIX application is the Intellution WorkSpace since it puts the most load on the network.

Objects in an operator display update by polling the OPC server. Each animated object has a configurable refresh rate. This rate determines how often each link requests the current value from the OPC server. When the OPC server is an iFIX SCADA server, object update rates are grouped together and sent as one transaction, up to 16 kilobytes at a time. If the request or response for that group exceeds 16 kilobytes, it is broken up into 16-kilobyte packets.

If more than one picture is open at the same time that has objects to the same SCADA server, there is a separate group for each picture.

When animated objects communicate with a third-party OPC server, data is sent and received according the server's requirements. Refer to your OPC documentation for more information.

Understanding Message Sizes

The actual message sizes transmitted by iFIX are dependent upon the type of objects in each picture.

Data links provide you with the option of requesting numeric or text data. Numeric data, the F_ fields, is always transmitted as floating point data and is four bytes in length. Text data, the A_ fields, is transmitted as the ASCII representation of the floating point value and is 12 bytes in length. One method to reduce the iFIX network load is to use only numeric data links.

Some special link types use data that is much larger than 12 bytes. For example, for each chart object, iFIX transmits approximately 180 bytes.

Alarm Summary objects have their own refresh rate which control how often they are updated. By increasing the values for the alarm refresh and data refresh rates you can fine-tune when iFIX reads data from its alarm queue and displays it.

Understanding Alarm Transfer

Alarm conditions are detected by the Scan Alarm and Control (SAC) program that runs on each SCADA server. The SCADA server sends an alarm message to each node in the network when an alarm is detected. Each alarm is over 1024 bytes in length. The actual message size transmitted by the SCADA server is slightly larger. If several alarms are detected in the same scan cycle, the SCADA server groups as many alarms as possible into a 16 kilobyte message before distributing the alarms to each node.

Optimizing iFIX to Reduce Network Traffic

You can optimize iFIX and reduce network traffic by using the following techniques:

- Use only the objects you really need. If you need more information, create a hierarchy of pictures. Put the objects that give conditional information in a separate picture and only open that picture when those conditions occur.
- Use numeric values (F_) instead of text values (A_). In addition to putting more information on the network, requests for ASCII values also increase the work that the SCADA server must do since the floating point to ASCII conversion is done on the server.
- Minimize the number of different object refresh rates.
- Increase the object refresh rates to decrease the update frequency. For more information on changing the refresh rate, refer to the section *Increasing the Refresh Rate.*
- Minimize the use of chart objects.

Working with Configurable Session Timers

The following conditions can cause iFIX to temporarily lose a session:

- Running iFIX over a network that contains slow communication links (less than 256Kbps).
- Opening a picture containing many objects on the SCADA server while other iFIX nodes are requesting data from the SCADA server. In this case, the iFIX network task does not get the CPU time that it needs because other programs are competing for CPU resources.

Both of these cases can be solved by increasing the timer values that iFIX uses. These timer values are referred to as configurable session timers.

Understanding iFIX Session Timers

iFIX uses network session timers to determine that another node is no longer running. Time-out values for every session-oriented message transfer are defined by iFIX when the session is established.

The four time-out values are described below:

Send — defines the amount of time that an iClient waits for a request to the SCADA server to be acknowledged. If this timer expires, the session ends.

Receive — defines the amount of time that an iClient waits for a reply from the SCADA server. When running iFIX over TCP/IP, the effective session time-out value is either the Send timer or the Receive timer, whichever is greater. If this timer expires, the session ends.

Keep Alive — defines the amount of time that, if no activity has occurred over an established connection, an iClient waits before sending a heartbeat message.

Inactivity — defines the amount of time that, if no data activity has occurred over an established dynamic connection, an iClient waits before removing the dynamic connection from the list of outgoing connections. If this timer expires, the session ends.

Determining Session Timer Values

It is important to choose your session time-out values correctly for your application. Values that are too low may cause sessions to be lost even though the remote node is running. Values that are too high may delay session problem notification. When considering what timer values to use, note that the Intellution WorkSpace may appear to be hung for up to the entire time-out period when sessions are lost. In production facilities, this delay may not give operators sufficient time to react to emergency situations.

For most applications, the default session time-out values are adequate. If you must modify the values to correct transient session losses, use this section to determine the correct values for your application.

iFIX uses the same session time-out values for every session. Changing the session timers affects sessions with every node in your iFIX network. In order to change the session timers, the changes must be made to every iFIX node.

You can also define remote node connection timers for each remote node defined in the SCU. The connection timers are identical to the session timers except that they affect communication with a particular remote node. Typically, the connection timers are used in place of the system-wide session timers when the connection to a remote node differs from the rest of the network. If you need to change these timers, make sure that the computers on both sides of the connection use the same timers.

Configurable session timers can be increased to solve the problems described at the beginning of this section. If you decide to change the values, it is recommended that you increase the Send and Receive values by 10 seconds and test to see if the problem is solved. If the problem persists, repeat the process until the problem is solved.

Configuring Session Timers

Session timers are configured in the SCU. You should only change session time-out values if you absolutely must, and only when you have a complete understanding of the implications.

For more information using the SCU, refer to chapter *Configuring iFIX Using the SCU*.

Working with Wide Area Networks

iFIX works equally well in a wide area network environment as it does in a local area network. However, if you use a wide area network, Intellution recommends that you use TCP/IP as the network software. TCP/IP is especially suited to wide area networks.

If you need to use iFIX in a wide area network over NetBIOS, note that different vendors' products work differently. One vendor's NetBIOS may work better in a WAN environment than another. NetBIOS typically transmits broadcast messages when iFIX registers the local node name on the network and when attempting to establish a session with another iFIX node. Broadcast messages can be disruptive in WAN environments.

The following list provides some methods to minimize the effect of NetBIOS broadcasts:

- Use iFIX on a single LAN segment prior to using node to node communications over a WAN.
- Start your SCADA server prior to starting your iClient. This minimizes the number of session establishment attempts from the iClient.
- Only list on-line SCADA servers in the Network Configuration dialog box of the System Configuration Utility.
- Minimize the number of broadcasts sent for each session establishment attempt by changing configuration parameters within the NetBIOS itself.
- Make sure that your WAN router product is optimized for your vendor's NetBIOS protocol.

Providing Remote Access

You have several choices for enabling computers at separate geographic locations to communicate with each other. Among these choices are remote control and remote access programs.

Understanding Remote Control Programs

Remote control programs take total control of a remote computer and send the remote computer's entire screen over a modem, which can result in slow performance. Note that the screen on both computers is the same. Keystrokes and mouse movements that you make locally are mirrored at the remote computer.

Understanding Remote Access Programs

Remote access programs, like Microsoft's Remote Access Service (RAS), treat a node that is located at a different geographic site as if it were on the local network. Only real-time process data is transferred over the modem. Remote access is usually more appropriate for remote monitoring of iFIX systems.

Microsoft's RAS does not require a dedicated computer to act as a gateway. Many other remote access products require some kind of dedicated computer to perform the gateway function between the LAN and the asynchronous line.

Understanding Remote Access Service

Microsoft's Remote Access Service (RAS) provides NetBEUI and TCP/IP over phone lines by treating your modem as a network adapter. NetBIOS and TCP/IP applications that run over a network can run over a serial connection. iFIX can use the NetBEUI and TCP/IP interface provided by RAS to communicate with other iFIX nodes over asynchronous lines.

RAS client and server software are standard with Windows NT 4.0 and Windows 2000. In general, a RAS client node dials into a RAS server node. A RAS client can dial in and access resources on a Windows NT or Windows 2000 RAS server's network. The Windows NT Workstation RAS server software allows one RAS client. Windows NT 4.0 and Windows 2000 software allows multiple RAS clients to be connected simultaneously.

Although RAS allows up to 256 clients to dial into a server simultaneously, the practical limit when RAS is used with the iFIX is significantly less. This is due to the additional resources that iFIX requires to communicate. Each simultaneous connection requires a separate modem on the server. Before you incorporate RAS into your production environment, it is strongly recommended that you test the configuration using multiple connections.

Using iFIX in conjunction with a RAS server provides the following capabilities:

- Alarm Summary objects are available.
- Data and alarms are available with one pair of modems.
- Access to the Alarm Startup Queue is available.
- File transfer using Microsoft networking over RAS is available.
- Multiple remote nodes can dial into a server simultaneously.

Use the following guidelines when incorporating RAS into your iFIX network:

- Only use modems with a minimum speed of 9600 baud. Verify that when the RAS connection is made that the modems are connected at a high speed. The faster the baud rate, the better performance you can expect.

- Use the Port Status on both the RAS client and server to troubleshoot connection problems and monitor ongoing communication. Refer to the RAS documentation for more information on using Port Status to troubleshoot communication.

- When browsing on the RAS client to access a remote SCADA server, you can improve performance by copying the file, *nodename*.TAG, from the SCADA server's PDB path to the View client's PDB path.

- Follow the steps below to allow a RAS client to dial into a Windows NT or Windows 2000 RAS server and access other iFIX nodes. Note that these steps apply only to iFIX running over NetBEUI.

  On the RAS server:

  [a] Set the RemoteListen parameter in the registry to 2. If you are running Windows NT 4.0 or Windows 2000, refer to the section *Modifying the Registry* for more information.

  [b] NBTASK.EXE cannot correctly determine the set of available LANAs only when:

  - You are running Windows 2000.
  - You are using NetBIOS for iFIX networking.
  - RAS Server Service is installed on the SCADA node.

  NBTASK fails to detect the LANAs used by RAS server. You must specify those LANAs on the command line to NBTASK.exe.

  For example, if the RAS server is using LANA 8 and LANA 9, you need to change the command line to NBTASK.exe in the FIX.ini file, located in the Dynamics\local directory, to the following:

```
[NETWORK]
RUN=%NBTASK.EXE /a8 /a9
```

The /a8 and /a9 were added to instruct NBTASK to detect incoming messages on LANA 8 and LANA 9.

You can download LANACFG.EXE, a utility used to determine and configure LANAs, from the Microsoft website. This utility can help you determine the LANA numbers that are used by the RAS Server Service.

On the RAS client:

Increase the refresh rate for all objects in your pictures to 3 seconds or greater. Refer to the section *Increasing the Refresh Rate* for more information.

Modifying the Registry

To edit the registry of the Windows NT RAS Server, do the following:

[1] Run the Registration Editor from the SYSTEM32 directory by typing the following from the command line:

```
REGEDT32
```

[2] Change the following registry value on the Windows NT RAS server node to 2 for NetBIOS bridging to work:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Re
moteAccess\Parameters\NetBIOSGateway\RemoteListen
```

To edit the registry of the Windows 2000 RAS Server, do the following:

[1] Run the Registration Editor from the SYSTEM32 directory by typing the following from the command line:

```
REGEDT32
```

[2] Change the following registry value on the Windows 2000 RAS server node to 2 in order for NetBIOS bridging to work:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
RemoteAccess\Parameters\Nbf\RemoteListen
```

Increasing the Refresh Rate

To increase refresh rate of an object:

[1] Double-click the object you want to modify.

[2] Click the Browse button to the right of the Data Source field.

[3] In the Refresh Rate field, click the drop down menu and choose a rate number that is smaller than your current refresh rate.

[4] Switch to the run-time environment, to make sure sessions are not lost and that alarms are received in a timely manner.

If sessions are being lost or alarms are not received in a reasonable amount of time, increase the refresh rate in 1 second increments until sessions are not lost and alarms are received without delay.

RAS Examples Using iFIX Over NetBIOS

To help illustrate the data and alarm transfer capabilities of iFIX, examples for each type of RAS communication are provided. RAS communications types are:

- Point to Point
- Point to LAN
- LAN to Point
- LAN to LAN

In each case, NODE A is a RAS client and NODE B is a RAS server.

Example: Point to Point

The following illustrates remote access communication between two standalone iFIX nodes. *Table 10-1* illustrates the communication capabilities of RAS in this scenario.

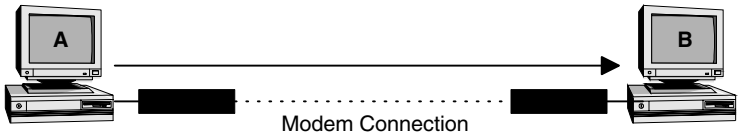


Figure 10-1: Understanding Point to Point Communication

Table 10-1: Point to Point Communication

Node	Can Receive Data and Alarms From Node...
A	B
B	A

Example: Point to LAN

The following figure illustrates a remote standalone node (A) dialing into a node (B) in a LAN. *Table 10-2* shows the communication available in this scenario.

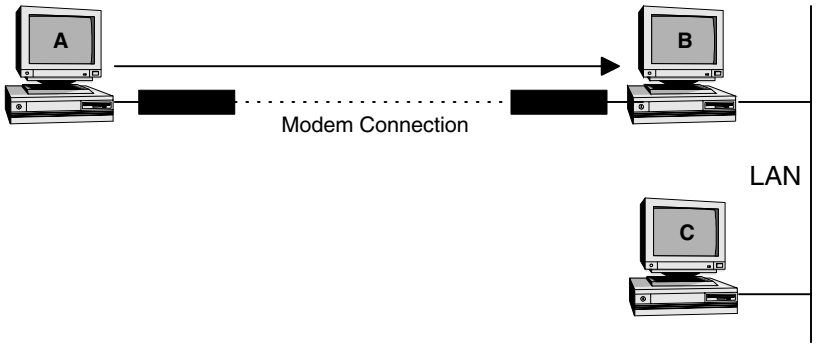


Figure 10-2: Understanding Point to LAN Communication

Table 10-2: Point to LAN Communication

Node	Can Receive Data and Alarms From Nodes...
A	B,C
B	A,C
C	A,B

Example: LAN to Point

The following figure illustrates a networked node (A) dialing into a remote standalone node (B). *Table 10-3* lists the access communication capabilities using RAS in this scenario.

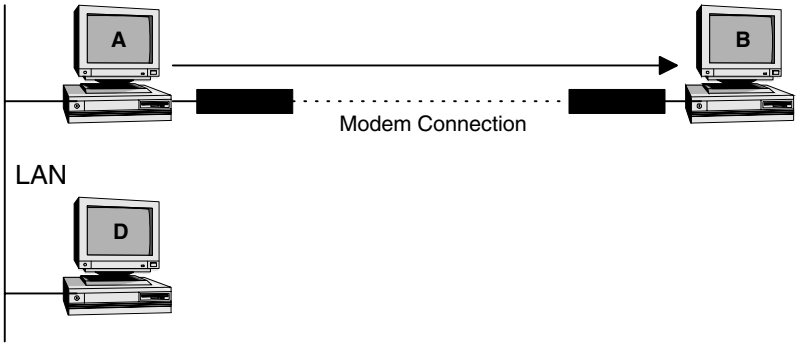


Figure 10-3: Understanding LAN to Point Communication

Table 10-3: LAN to Point Communication

Node	Can Receive Data and Alarms From Node...
A	B
B	A
D	None

Example: LAN to LAN

The following figure illustrates communication between two LANs. *Table 10-4* lists the communication between two LANs using RAS. A more appropriate solution for this type of communication would be a WAN with dedicated routers.

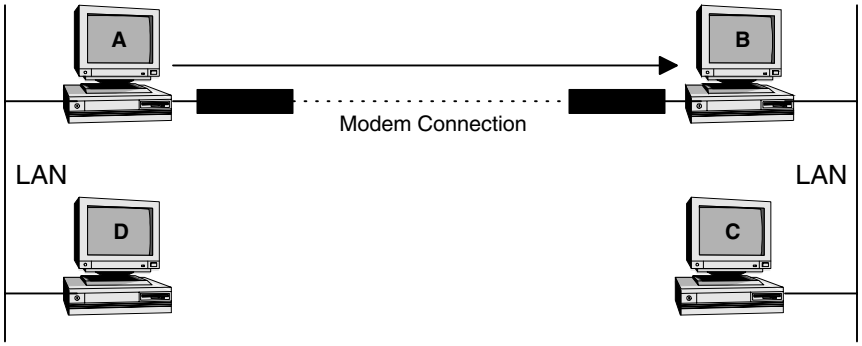


Figure 10-4: Understanding LAN to LAN Communication

Table 10-4: LAN to LAN Communication

Node	Can Receive Data and Alarms From Nodes...
A	B,C
B	A,C
C	A,B
D	None

Network Paths

As described in the chapter *Getting Started*, iFIX supports NetBIOS and TCP/IP network protocols. If an iClient should lose its connection to another node, the local computer attempts to re-establish its connection over all available network paths in parallel.

The computer's network protocol determines the specific network paths. For example, when the computer uses NetBIOS, all LANA numbers containing NetBEUI are valid network paths. LANA numbers associated with RAS are also valid but will not start a RAS connection. If there is no RAS connection at the time that the computer tries to connect, the attempt for that path fails.

When the computer's protocol is TCP/IP, each IP address is a valid path. IP addresses bound to RAS are also valid but will not start a RAS connection. If there is no RAS connection at the time of the computer tries to connect, the attempt for that address fails.

The first successful connection is the one that the iClient uses. Although you cannot specify which network path to use, you can exclude network paths in the SCU. For more information about using network paths, refer to the section *Understanding LAN Redundancy* in the *Mastering iFIX* manual.

By default, iFIX enables all available network paths. You can disable any network path you do not want to use. If you subsequently discover you need the path, you can re-enable it later.

Integrating iFIX into Your Network

You may have communication requirements in addition to iFIX communications that must be considered. These network and communication requirements fall into the following categories:

- Additional network software required by the I/O driver you are using.
- File server communication software to allow central storage of data files.
- Relational database communication software.

Integrating solutions to each of these requirements can be a difficult task. Intellution recommends that you ensure that all the software required to address these requirements works together.

Disabling Connections from Unauthorized Nodes

By default, iFIX nodes accept connections from any remote node over TCP/IP or NetBIOS, given adequate resources. However, you may want to prevent unknown or unauthorized nodes from obtaining a connection to a SCADA server by entering specific settings into a network initialization file called NETWORK.INI. This file contains a parameter, accept_unknown_host, which controls whether the SCADA server accepts connections from other computers.

When the parameter is set to ON, the SCADA node accepts connections from any computer. However, when the parameter is set to OFF, access is restricted to the View clients you specify. The exact nodes that can access the SCADA server are defined by listing them in the NETWORK.INI file using the following syntax:

```
hostn=nodename
```

For example, to provide access for the iClients, View01 and View05, to a remote SCADA server, your NETWORK.INI file on the SCADA server should be:

```
[TCPIP]
accept_unknown_host=OFF
host1=VIEW01
host2=VIEW05
```

Later, if you want to restrict access to only View01, you can remove the View05 line from the file. Likewise if you want to provide View04 access to the SCADA server, you can add the following line to the file:

```
host2=VIEW04
```

Notice that View04 is given the same host number that View05 had. This is necessary because all host numbers must be consecutive. For example, you cannot define host1 as View01 and host3 as View04 unless host2 is already defined in the file.

To restrict access to a SCADA server:

[1] In a text editor, type the following:

```
[TCPIP]
accept_unknown_host=OFF
```

[2] Add the View clients that can access the local SCADA node.

[3] Save the file as NETWORK.INI. Make sure you save the file to the FIX Local path on the SCADA server.

Disabling Database Write Access for Unauthorized Nodes

By default, iFIX SCADA servers accept database write requests from any remote node. However, you may want to prevent unknown or unauthorized nodes from writing to a SCADA server by entering specific settings into the server's network initialization file, NETWORK.INI. This file contains the parameter accept_unauthorized_writes, which controls whether the SCADA server accepts database writes from iClients.

When the accept_unauthorized_writes parameter is not present in the NETWORK.INI file or set to ON, the SCADA server accepts write requests from any computer. When the parameter is set to OFF, access is restricted to the View clients you specify regardless of who is logged into the remote nodes. The exact nodes that can access a SCADA server's database are defined by listing them in the NETWORK.INI file using the following syntax:

```
writenode#=nodename
```

For example, to provide access for the View clients, VIEW01 and VIEW05, to a remote server, configure your server's NETWORK.INI file as follows:

```
[WRITEACCESS]
accept_unauthorized_writes=OFF
writenode1=VIEW01
writenode2=VIEW05
```

If you subsequently want to restrict database access to VIEW01 only, you can remove VIEW05 from the file. Likewise, if you want to provide VIEW10 access to the SCADA server's database, you can add the following line to the file:

```
writenode2=VIEW10
```

Notice that VIEW10 is assigned the same number that VIEW05 had. This is necessary because all node numbers must be consecutive. You cannot define writenode1 and writenode3 without also defining writenode2.

SCADA Server Failover

When you use this feature in conjunction with SCADA server failover, the NETWORK.INI file on each of the SCADA nodes must have their partner SCADA node listed to enable alarm acknowledgement synchronization.

For example, if you have two partner SCADA nodes, SCADA1 and SCADA2, then the NETWORK.INI file for SCADA1 should be:

```
[WRITEACCESS]
accept_unauthorized_writes=OFF
writenode3=SCADA2
```

The NETWORK.INI file for SCADA2 should be:

```
[WRITEACCESS]
accept_unauthorized_writes=OFF
writenode3=SCADA1
```

Disabling the Logging of Unauthorized Writes

When the accept_unauthorized_writes parameter is OFF, the SCADA server treats all failed (unauthorized) write attempts as operator alarms and records these write attempts to all the alarm destinations enabled on the SCADA server. Using the

parameter log_unauthorized_writes, you can disable the logging of failed writes by setting the parameter to OFF. When the parameter is not present in the NETWORK.INI file or set to ON, the SCADA logs all unauthorized write attempts.

To disable logging of unauthorized writes, configure your NETWORK.INI file as follows:

```
[WRITEACCESS]
accept_unauthorized_writes=OFF
log_unauthorized_writes=OFF
writenode1=VIEW01
writenode2=VIEW10
```

Once you create or modify the NETWORK.INI file, you changes take effect immediately.

You can also restrict database write access by assigning security areas to specific groups and users. For more information about security areas and how to use them with the accept_unauthorized_writes parameters, refer to the *Implementing Security* manual.

To restrict database write access to a SCADA server:

[1] Open the NETWORK.INI on your SCADA server using a text editor. If available, this file resides in the iFIX Local path. If the file does not exist, create it in the iFIX Local path with your text editor.

[2] Enter the following text:

```
[WRITEACCESS]
accept_unauthorized_writes=OFF
```

[3] Add the following text if you want to disable the logging of unauthorized writes:

```
log_unauthorized_writes=OFF
```

[4] Add the View clients that can access the local SCADA server. Use the format:

```
writenode#=nodename
```

[5] Save the file and make sure the file resides in the iFIX Local path.

Configuring SCADA Server Failover

iFIX uses logical node names to allow you to establish SCADA server failover in your network. Logical node names are specified in the SCU. The following example illustrates the use of logical node names in configuring SCADA server failover using the SCU. For detailed information on establishing SCADA server failover throughout your iFIX environment, refer to the *Mastering iFIX* manual.

Let's say you want to configure SCADA server failover in your packaging network, such that an iClient, UTIL_V1, automatically reconnects to a backup SCADA server, PACKER2, should the primary SCADA server, PACKER1, fail. To do this, configure SCADA server failover using the SCU on the iClient:

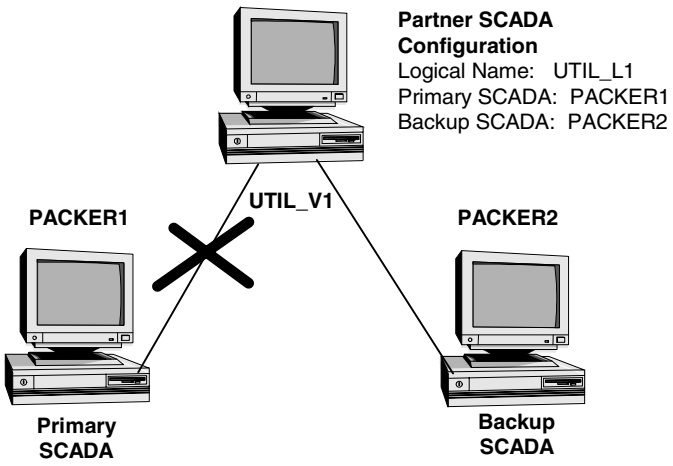
[1] In the Local Startup Definition dialog box, enter the local node name PACKER1 and set a local logical name (UTIL_L1) in the appropriate fields on both SCADA servers.

[2] On your iClients:

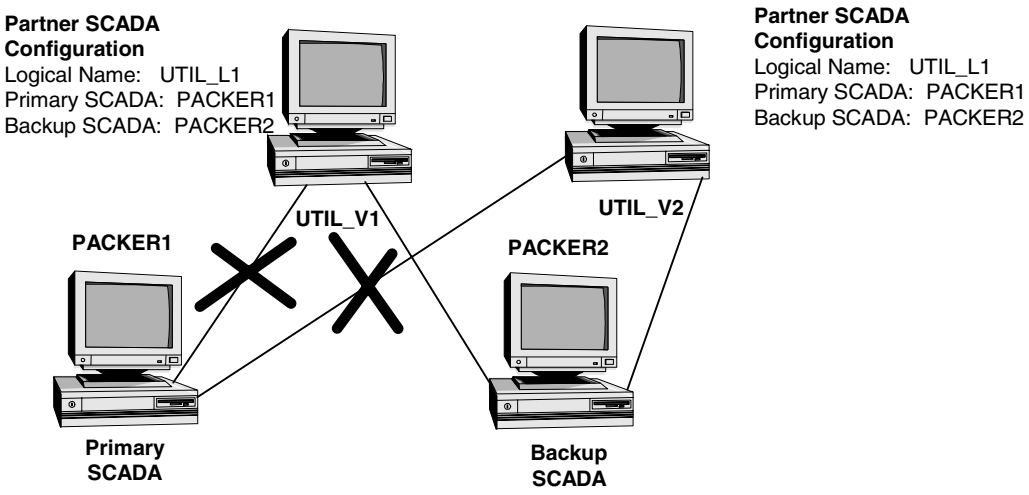
  [a] In the Network Configuration dialog box, enter UTIL_L1 in the Remote Node Name field, and add the name to the Configured Remote Nodes list. Click Configure.

  [b] In the Remote Node Configuration dialog box, select Enable Logical Node Names, and enter PACKER1 as the primary node and PACKER2 as the backup node in the appropriate fields.

By performing the previous procedure, you have configured a logical node, UTIL_L1, that groups both your primary and backup SCADA servers, PACKER1 and PACKER2. The iClient, UTIL_V1, establishes connection with this logical pair, not the individual server. Therefore, if the connection to PACKER1 is lost, UTIL_V1 automatically fails over to PACKER2 and re-establishes communication. This is illustrated below.



To expand your SCADA server failover to include additional iClients, you could establish another iClient, UTIL_V2, configured with a Local Logical Name of UTIL_L1. In this scenario, UTIL_V2 can also retrieve data from PACKER2 if PACKER1 fails, because it is attached to logical node name UTIL_L1. This is illustrated below.



SCADA server failover in iFIX ensures that the client is always operable should there be a node or network failure. Using the SCU, you can easily configure this important feature in your process environment.

11. Troubleshooting

iFIX provides an extremely secure software interface for controlling your process. Certain conditions, however, such as insufficient memory and computer failure, can cause problems when your system operates. This chapter provides descriptions of these and other typical problems operators may experience. It also lists potential courses of action that you can take to quickly resume normal operation.

Overview

Two key characteristics of your operating system that you must consider if problems occur while iFIX is running include:

Multi-tasking — allowing the operating system to run several applications simultaneously.

Memory management — handling the usage of RAM and, in the case of virtual memory, hard disk space.

Your operating system provides the Control Panel to configure these characteristics. If components within the Control Panel are not configured correctly, your computer may behave strangely or stop working.

Understanding the Control Panel

Your operating system's Control Panel lets you set up the following computer components:

- Video driver
- Network card
- Mouse
- Keyboard
- System (used to set up virtual memory)
- Drivers (used to set up sound boards and the timer driver)
- Services

These configuration components are critical to troubleshooting insufficient memory and computer failure problems. Instructions for accessing and implementing changes to these components are provided in your operating system's documentation.

Avoiding Problems

You can avoid problems by configuring your system properly before operation. When troubleshooting, always try to simplify your system and remove any unnecessary hardware or software.

The following list is the minimum recommended configuration you should adhere to while troubleshooting problems:

- Use Intellution-recommended computers, as described in the section *Recommended Computers.*
- Use Intellution-recommended network hardware and software, as described in the chapter *Networking iFIX Nodes*.
- Use standard video adapters and drivers.
- Avoid using the power-saving feature that can be configured on some computers.

Make sure that all iFIX nodes comply with these recommendations.

Computer Failures

Computers can sometimes stop working without warning. In these cases, the computer may or may not display error messages to help you determine what happened. These failures can be caused by:

- Memory conflicts between two or more drivers.
- Wrong network driver versions.
- Incorrect operating system setup information.
- Old 3COM network cards.

Troubleshooting Computer Failures

If you experience computer failures, try to resolve them using the tips below:

- If you are using a 3COM network card, verify that the card is a 3C905 or 3C509.
- See what other boards may be in the machine, such as a video board or a memory-resident interface card. Find out the memory addresses and interrupts that these boards are using and resolve any conflicts.
- If you have a network card installed, make sure that it is listed in the Control Panel.

Problems with Establishing or Losing Sessions

You can lose communication sessions because your network times out. These time-outs usually occur on the client side of a session. The primary reason for time-outs is that iFIX network tasks on the SCADA server or iClient did not get enough CPU time to service a request.

NOTE: *Network sessions may be lost when you open large pictures.* iFIX *re-establishes the session after the picture finishes opening. To eliminate this problem, use the information in the section Working with Configurable Session Timers.*

The following factors prevent the network task on the SCADA server or iClient from getting enough CPU time:

- Heavy disk activity.
- Large picture calculation time.
- SAC running to completion when database overruns occur.
- Database Manager sorting.
- Historical Collect closing and starting a new file.
- Other applications, such as Intellution WorkSpace, Historical Collect, and Database Manager, taking time-slices before data can be processed.

Troubleshooting Session Loss

If you are using NetBIOS, run the tests described in the section *Troubleshooting NetBIOS with NBTEST*. If you are using TCP/IP, use the information in the section *Troubleshooting TCP/IP*.

Troubleshooting Networks

If you are experiencing network problems while trying to run iFIX, use the following steps to identify the problem area:

[1] Refer to the chapter *Networking iFIX Nodes* to ensure that the network hardware and software are properly configured. Unless otherwise indicated, it is recommended that you use the latest version of your chosen network software.

[2] Verify that the network software itself is working properly prior to running any iFIX programs. Use the troubleshooting information in the section *Troubleshooting Microsoft Networking* to confirm that the network is working correctly. In addition, if you are using TCP/IP, use the PING program described in the section *Troubleshooting TCP/IP* to ensure the network is operating properly.

[3] Test your network connection:

  [a] If you are using NetBIOS, use NBTEST to verify that connections can be established. Refer to the section *Troubleshooting NetBIOS with NBTEST* for instructions on using this program.

  [b] If you are using TCP/IP, use TCPTEST diagnostics described in the section *Troubleshooting TCP/IP* to verify that the network is working correctly.

[4] Use the error codes in the section *Network Error Codes* to modify iFIX configuration if you continue to have problems keeping iFIX sessions active.

[5] Use Intellution's Network Diagnostics program, NETDIAG, from the Program Manager. This program creates the file, NETDIAG.DAT, in the Application path. This file can be sent to Intellution's Technical Support Department for further assistance.

Troubleshooting Microsoft Networking

If you experience network problems with iFIX, verify that the network software is loaded and working properly. The test described in this section must work in order for iFIX networking to function properly. This test uses the file sharing capabilities inherent in Microsoft networking to test the network. You do not need to start iFIX in order to run this test.

Use the following steps to test communications between two nodes that are running Microsoft Windows:

[1] Start both computers.

[2] Enable file sharing on each computer. See your operating system's documentation for more information on how to configure file sharing.

[3] Define a shared directory on each computer. See your operating system's documentation for information on sharing a directory.

[4] Configure a network drive, for example D:, on each node that points to the shared directory on the other computer. Click the Map Network Drive button (available on the toolbar of any window) to select the shared directory configured in step 3.

This test must run successfully. If it does not, refer to the chapter *Networking iFIX Nodes* and ensure that the network is configured properly.

Troubleshooting NetBIOS with NBTEST

If you have trouble starting iFIX because of networking problems or you are having problems establishing sessions, verify NetBIOS itself is loaded and working properly. Intellution provides a test program, NBTEST, to help you verify that NetBIOS is working. Note that even if NBTEST succeeds, it does not necessarily mean that iFIX is compatible with your network's NetBIOS implementation. However, NBTEST must pass in order for iFIX to communicate properly.

The NBTEST executable file (NBTEST.EXE) is installed into the FIX Base path when you install iFIX. It is recommended that NBTEST be executed without iFIX running because it may interfere with iFIX communications. Before you run the program,

Run NBTEST using the Run command from the Start menu. Running the program without parameters provides you with instructions. You can display extended help by typing the following command:

```
NBTEST /h<Enter>
```

NBTEST uses LAN adapter 0 by default. Before you run the program, make sure that NetBEUI on your SCADA server and View client use this LAN adapter. You can determine the LAN adapter used by each computer with the Network control panel.

If the server and client are not using LAN adapter 0, you can change the LAN adapter that NBTEST uses by typing the following command:

```
NBTEST /annn<Enter>
```

For example, if the SCADA server uses LAN adapter 1, type the following command to start NBTEST:

```
NBTEST /a1<Enter>
```

NBTEST runs in one of two modes. Mode 1 tests that two computers can exchange information over the NetBIOS interface. Mode 2 tests that two computers can exchange information for an extended period with acceptable performance.

Exchanging Data Over NetBIOS with NBTEST Mode 1

Mode 1 tests if two computers can exchange information over the NetBIOS interface in a manner similar to iFIX. In this test, one computer is considered a *client* and the other a *server*. This test performs the following tasks:

[1] Adds the NetBIOS names.

[2] Establishes a client to server session.

[3] Exchanges data over the client to server session.

[4] Establishes a server to client session.

[5] Exchanges data over the server to client session.

[6] Terminates both sessions.

To run NBTEST in test mode 1, you must run the program on two different computers. One computer is defined as a server node using the command:

```
NBTEST /s
```

The second node is defined as a client node using the command:

```
NBTEST /c
```

This test runs for approximately 30 seconds. A successful test displays the following message on each computer:

```
SUCCESS!
```

If this test is not successful, resolve the first error you see on the screen and rerun the test until it is successful. Refer to the chapter *Networking iFIX Nodes* to configure your network hardware and software for use with iFIX.

Exchanging Data Over NetBIOS for an Extended Period with NBTEST Mode 2

Mode 2 tests if two computers can exchange information for an extended period with acceptable performance. This test performs the following tasks:

[1] NetBIOS names are added.

[2] The client establishes a session with the server.

[3] Data is exchanged until a key is pressed on either computer.

To run NBTEST in test mode 2, you must run the program on two different computers. One computer is defined as a server node using the command:

```
NBTEST /s
```

The second node is defined as a client node using the command:

```
NBTEST /c /f
```

Once the session is established, the client sends a 1400-byte request to the server. The server sends back a 1400-byte reply. A dot appears on screen for each request and reply pair. In general, 5-10 dots appear on the screen per second. If the rate is less, this implies there is a performance bottleneck in the NetBIOS software itself.

Stop the test by pressing a key on either computer. If pressing a key does not stop the test, there is a problem within the NetBIOS interface.

Setting the Buffer Size

With the /b command, you can set the receive and send buffer size. For example, the following command sets the buffer size to 16K:

```
NBTEST /b16384<Enter>
```

The default buffer size is 1400. If you use this command, make sure both the client and the server have the same buffer size.

Troubleshooting TCP/IP

If you experience difficulty establishing network communications, your TCP/IP software and the iFIX TCP/IP network software provide some utilities to help locate the cause of the problem. These utilities are described in the following sections.

Using PING

PING is a TCP/IP diagnostic utility that helps to isolate network hardware problems and incompatible configurations by allowing you to verify a physical connection to a remote computer. PING must run successfully before iFIX can run properly. To run PING, type the following from the command line:

```
PING SCU_nodename<Enter>
```

For example, to test a connection from a View node to the local SCADA node, SCADA01, type the following:

```
PING SCADA01<Enter>
```

See your TCP/IP manuals for additional information on using PING.

Working with TCPTEST

Another utility, provided by Intellution, is the TCPTEST diagnostic program. To run TCPTEST, select the Run command from the Start menu and type the following into the command line:

```
TCPTEST parameters <Enter>
```

where *parameters* are one or more of the following command parameters in the table *Table 11-1*. To display a list of parameters on the screen, type the following:

```
TCPTEST <Enter>
```

The program requires two nodes to run, one as a client and one as a server. Set up the server node first, as follows:

```
TCPTEST /S <Enter>
```

The client node must use as a minimum the following TCPTEST parameters:

```
TCPTEST /C /Rnodename <Enter>
```

where *nodename* is the SCU node name of the server node. For example, to make VIEW01 a server, run TCPTEST with the /S parameter, as shown above. To communicate with VIEW01, go to another node and type the following:

```
TCPTEST /C /RVIEW01 <Enter>
```

Table 11-1: TCPTEST Parameters

The parameter…	Lets you…
/B*x*	Set the receive and send buffer size to *x*. The default size is 1400 messages. If you specify this parameter, make sure that both nodes have the same buffer size.
/C	Set up a node as a client. This parameter requires you to provide the remote server node name (see the /R parameter below).

Table 11-1: TCPTEST Parameters

The parameter…	Lets you…
/D	Display run-time information (such as the data received).
/F*x*	Set to *x* milliseconds, how often to send messages. By default, messages are sent as fast as possible.
/P*portnumber*	Use *portnumber* in place of the default ports for both the server node and the client node.
/R*server*	Specify the name of the remote server node.
/S	Set up this node as a server.
/T*x*	Set the TCP time-out value for sending and receiving data to *x*. This parameter is supported only if your WINSOCK implementation supports changing the TCP time-out value. Most implementations do not.
/W	Test the WINSOCK interface and display WSAData (for example, vendor information).

Intellution recommends you run TCPTEST without iFIX running. If you need to run both at the same time, be sure to change the port number (/P) that TCPTEST uses. Otherwise, a conflict may occur with the data being passed because, by default, TCPTEST uses the same port number as iFIX. Note that the client and server must use identical port numbers when using TCPTEST.

Working with NETDIAG

NETDIAG provides comprehensive network diagnostic information and stores its information in the file NETDIAG.DAT. This file resides in the Application path.

To run NETDIAG, select Run from the Start menu and type the following on the command line:

```
NETDIAG<Enter>
```

Network Error Codes

The following sections list the error codes, messages, and explanations for the network errors you can encounter if you experience problems with your network.

Startup Error Codes

If a network problem occurs during startup, one of the error codes or messages listed in the following table may appear.

Table 11-2: Startup Error Messages

Error Code	Error Message	Description
1613	Duplicate name in local name table.	A name conflict exists in the Local Name Table within NetBIOS. Examine the names added by third-party networking software to find the source of the conflict. This error can also occur if iFIX did not shut down properly prior to starting back up. In this case, restart the computer and iFIX.
1622	Name in use on remote node.	The node name assigned to the node is currently in use on another node. Rename one of the nodes to correct this conflict.
8501 8502	Underlying network subsystem not ready. TCPTASK: Failed to initialize network subsystem.	TCP/IP is not installed properly or is missing. Use PING or TCPTASK to verify that the underlying TCP/IP is set up before attempting to run iFIX.
8503	Windows Sockets API version mismatch.	When attempting to initialize the Winsock TCP/IP interface, TCPTASK detected that the Winsock version is less than 1.1. To correct the problem on Windows NT, make sure that Service Pack 3 or higher is installed. Service Pack 6 is recommended for iFIX.

Run-time Error Codes

If a network problem exists that prevents sessions from establishing or causes sessions to be terminated, one of the error codes listed in the following table may appear in the NETDIAG program.

Table 11-3: Run-time Error Codes

Error Code	Error Message	Description
1605 1608 1610 1624	Command timed out. Invalid Local Session Number. Session Closed. Session Ended Abnormally.	These errors occur when the remote node is down. When the remote node is brought back up, the Connection Manager re-establishes the session.
1620	Can't find name called.	The session cannot be established because either a remote node is not operating, a cabling problem exists between the nodes, or the remote node name is not registered on the network. Verify both nodes are running compatible network software. Also, run NBTEST as discussed in the section *Troubleshooting NetBIOS with NBTEST*.
1914	Connection NOT established with node.	The Connection Manager has not yet established a connection with the remote node. Wait for Connection Manager to establish the session.
1960	FIX dynamic connection in progress.	Connection Manager is in the process of establishing a dynamic connection with the remote node. Wait for Connection Manager to establish the session.

Table 11-3: Run-time Error Codes (continued)

Error Code	Error Message	Description
1964	FIX has been shut down on remote node.	Connection Manager has detected that iFIX has been shutdown on the remote node. This error code shows up temporarily and then changes to 1914.
8517	Node not found in TCP hosts database.	The node name that you are trying to connect to be resolved to an IP address. The name is probably not in the local hosts file or on the WINS server. Obtain the remote node's IP address and add it to the HOSTS file.

Troubleshooting the Auto Alarm Manager

After setting up the Auto Alarm Manager, you should test its operation to ensure it is working as you intended. The following section summarizes common problems you may encounter when using Auto Alarm Manager, and their possible solution(s).

When I start the SCU, I get the following message: Can't find RASAPI32.DLL.

Do the following:

[1] Install the Windows Remote Access Service software on your computer.

Mission Control displays the error 1618 whenever the Auto Alarm Manager sends an alarm.

The value for the registry parameter RemoteListen may be set to 1 on the receiving node.

Do the following:

[1] Change the parameter to 2. Refer to the *Modifying the Registry* section for instructions on how to change this value.

The modem on the receiving node does not hang up when the modem on the sending node does.

You may need to enable Hardware Flow Control and Modem Error Control in your RAS software. To do this, open the Network Control and do the following:

[1] Select Remote Access Service from the Install Network Software list box.

[2] Click Configure.

[3] Select the port your modem uses from the dialog box and click Configure.

[4] Click Settings.

[5] Click the Enable Hardware Flow Control and Enable Error Control check boxes.

[6] Close all the open dialog boxes, the Network Control Panel, and restart your computer to ensure that the changes take effect.

The RAS server cannot be added to the SCU task list so that it starts automatically with iFIX.

To start the RAS server automatically:

[1] Select Remote Access Server from the Services dialog box and click Startup. The Service dialog box appears.

[2] Click Automatic and close all the open dialog boxes and the Service Control Panel to save your changes.

[3] Restart your computer to start the RAS server automatically.

The Auto Alarm Manager fails to connect.

You need to specify the name of a Windows user account that has dial-in permission in the Advanced Send Alarm Settings dialog box. Refer to the *Configuring the Auto Alarm Manager* section in the *Implementing Alarms and Messages* manual for instructions.

Auto Alarm Manager Messages in Mission Control

The following table details possible messages that the Auto Alarm Manager may display during its operation, and lists potential solutions to the problem that the messages convey.

Table 11-4: Troubleshooting Auto Alarm Manager Messages

Message	Solution
Cannot find the phone book entry	The primary or secondary contact specified in the SCU is not defined in the RAS phone book. Create a phone book entry for each contact before continuing. Refer to your Microsoft manuals for instructions.
Hardware failure in port or attached device	The Auto Alarm Manager cannot communicate with the local modem. Verify that the cable connection between the modem and the computer is secure. If the problem persists, try a different cable or modem.
Cannot detect carrier	The Auto Alarm Manager could not establish a connection to the receiving node. Make sure the RAS server is running. Also make sure the local modem detects a dial tone when it dials the primary or secondary contact.

Table 11-4: Troubleshooting Auto Alarm Manager Messages (continued)

Message	Solution
ERROR_INTERACTIVE_MODE	Do the following: [1] Select the phone book entry you want to edit. [2] From the Remote Access dialog box, click Edit. Click Advanced. If the Basic button appears, proceed to the next step. [3] Click Modem. [4] Deselect the Enter Modem Commands Manually check box. [5] Close all open dialog boxes and exit the Remote Access program. The next time the Auto Alarm Manager dials, you should not receive an error.
Testing the connection… Connection BAD	After establishing RAS and iFIX connections, the Auto Alarm Manager on the sending node sent a test message to the receiving node and did not get a response. Make sure that Auto Alarm Manager is running on the receiving node. If it is not, start it.

Table 11-4: Troubleshooting Auto Alarm Manager Messages (continued)

Message	Solution
The account does not have remote access permission	The currently logged in user or the name of the user account specified in the Advanced Send Alarm Settings dialog box does not have the necessary rights to dial into the RAS server. Use the RAS Administrator program on the server node to grant dial-in rights to the necessary users.
All AAM session attempts failed	The Auto Alarm Manager could not communicate with the Auto Alarm Manager on the remote node. Make sure the following conditions exist: • The names of the primary and secondary contacts match the names of remote nodes associated with each RAS phone book entry. If they do not, edit the entries. Refer to your Microsoft manuals for more information. • The Auto Alarm Manager is started with the correct command line parameter on the sending and receiving nodes. Use the /c parameter on the sending node and the /s parameter on the receiving node. Refer to the *Implementing Alarms and Messages* manual for more information. • The sending and receiving nodes are not on the same LAN.

Index

A

AAM 86
  viewing statistics 88
advanced
  alarm configuration 57
alarm acknowledgement synchronization 86
  enabling 108
  viewing statistics 89
alarm areas
  common configuring 57
  configuring 52
  editing the database 58
Alarm ODBC 86
  viewing statistics 89
alarm queues
  modifying 58
alarm services
  customizing 52
  enabling 51
alarms
  configuring 51
  configuring alarm acknowledgement synchronization 61
  configuring areas 52
  configuring common areas 57
  configuring the Auto Alarm Manager 58
  customizing services 52
  deleting 56
  editing alarm area database 58
  enabling Alarm ODBC service 57
  enabling services 51
  formatting messages 55
  queues modifying 58
  transfer 93
Auto Alarm Manager
  configuring 58
  troubleshooting 126
  viewing statistics 88

B

background tasks
  iFIX functions 82
  specifying 63
backup
  file server files 12
  for SCADA servers in networks 110
base directory 40

C

computers
  components troubleshooting 114
  failures troubleshooting 115
  recommended for iFIX 5
Configuration file 2
configuring
  alarm acknowledgement synchronization 61
  alarm areas 52
  alarms 51
  Auto Alarm Manager 58
  common alarm areas 57
  I/O drivers 61
  iFIX nodes 31
  iFIX running as a service 47
  iFIX to run as a service under Windows 46
  LAN redundancy 50
  NetBEUI 26
  network connections 48
  network protocols 48
  network timers 51
  relational databases on iFIX 65
  remote nodes 49
  SCADA servers 60

SCU 43
security 48
startup tasks 62
TCP/IP 29, 31
connections
disabling from unauthorized nodes 106
establishing network 92
Control Panel
using to troubleshoot problems 114
customizing alarm services 52

D

data transfer 92
database write access
disabling 107
defining a common message format 57
demo mode
troubleshooting 19
DHCP/WINS
function 30
TCP/IP name resolution 29
disabling connections from unauthorized nodes 106
disabling database write access for unauthorized nodes 107
displays
updates to links 92
DNS 1
DNS server
function 30
TCP/IP name resolution 29
drivers
See I/O drivers
dynamic connections
described 49

E

editing alarm area database 58
enabling
alarm acknowledgement synchronization 108
alarm services 51
database access for SCADA server failover 108
SCADA support 60
events
formatting messages 55
exiting SCU 39
extended period 120

F

file servers
recommended 11

H

hardware
optional 12
requirements for iFIX 4
hardware key 1
described 6
installing 15
parallel port 15
parallel-port supported 6
replacing defective 21
troubleshooting 19
USB port 16
USB-supported 6
hardware requirements
recommended computers 5
HOSTS file, local
function 30
syntax 30
TCP/IP name resolution 29
HTC 86
starting and stopping 88

I

I/O control
datascope program 87
tuning driver period 87
tuning driver's message rate 87
what it allows you to do 85
I/O drivers
configuring 61
starting automatically 64
starting manually 87
iFIX
background tasks 82
configuring nodes 31
configuring relational databases 65
configuring remote nodes 49
configuring tasks to automatically start 62
dynamic connections 49
hardware requirements 4
implementing the SCU, list of general tasks 43

integrating into networks 106
memory management 113
memory requirements 6
multi-tasking problems 113
nodes, disabling connections 106
optional hardware 12
port assignments, verifying 31
recommended computers 5
recommended file servers 11
recommended video drivers 9
running as a service under Windows 46
running tasks in the background 63
session temporary loss 94
shutdown 81
software requirements 7
starting up 2
startup 77
startup options 81
Startup program 77
supported file servers 11
supported network software 11
supported networks 10
iFIX environment
setting up main tasks 1
tasks to complete prior to setup 3
tasks to complete to set up iFIX nodes 12
iKeyDiag
running 22
using 22
increasing the refresh rate 101

L

LAN redundancy
configuring 50
LAN-to-LAN communication
remote access example 104
LAN-to-point communication
remote access example 103
local
logical name specifying 45
server name specifying 45
startup options described 45
startup options specifying 45
Local Node Alias feature
described 48
enabling 48
Local Startup command
Configure menu 45, 46
logical node names 45

M

mapping IP addresses
using a TCP/IP network 29
memory management
possible cause of problems 113
memory requirements
iFIX 6
messages
application routing 57
defining a format 57
formatting 55
sent by iFIX 91
size 93
messaging
network 91
Microsoft networking
See networking
Microsoft RAS
See RAS
minimize after Startup
startup option 81
Mission Control
AAM tab 86
alarm acknowledgement synchronization 89
Alarm ODBC 89
Alarm ODBC tab 86
Alarm Synchronization tab 86
Auto Alarm Manager 88
background tasks monitored 85
closing 86
Historical Collect 88
HTC tab 86
I/O Control tab 85
SAC tab 86
SQL tab 86
starting 85
troubleshooting Alarm Manager messages 128
modifying alarm queues 58
multi-tasking
possible cause of problems 113

N

name resolution 29
NBTEST
exchanging data over NetBIOS 119
troubleshooting NetBIOS 118
NetBEUI 1
configuring 26

interface provided by RAS 98
required components 26
using 25
NetBIOS
establishing communication using 48
exchanging data over, NBTEST Mode 1 119
exchanging data over, NBTEST Mode 2 120
interface provided RAS 98
sessions 92
troubleshooting with NBTEST 118
using 25
working with WANs 96
NetBIOS and TCP/IP
switching between 34
NETDIAG
using to troubleshoot TCP/IP 123
network adapters
3COM Ethernet 25
Intel Ethernet 25
Network button
SCU toolbox 48, 49
network connections
configuring 48
dynamic 49
network error codes 124
run-time error codes 125
network load 91
network protocols
configuring 48
NetBEUI 25
TCP/IP 28
network timers
activating on a per-node basis 49
configuring 51
networking
Microsoft troubleshooting 118
networking with other iFIX and FIX nodes 35
networks
backup for SCADA servers 110
establishing connections 92
integrating iFIX into 106
messaging 91
session timers 94
sessions 91
setting up a distributed processing system 1
software supported 11
supported 10
traffic, optimizing iFIX to reduce 94
troubleshooting 117
nodes
configuring remote 49
disabling connections 106
disabling write access 107

O

optional hardware
iFIX 12
options
local startup 45

P

parallel port hardware key 15
path
descriptions 41
specifying for iFIX directories 40
PING
using to troubleshoot TCP/IP 121
planning
tasks to complete prior to setup 3
point-to-LAN communication
remote access example 102
point-to-point communication
remote access example 101
ports
selecting 55
verifying assignments 31
printer
naming 56
process database
defining the database to load when iFIX starts 60

R

RAS
described 98
editing the Windows 2000 Registry 100
editing the Windows NT Registry 100
examples using iFIX over NetBIOS 101
recovery for improper USB hardware key installation 18
registered tasks
startup option 81
relational database
configuring iFIX 65
remote access
LAN-to-LAN communication example 104
LAN-to-point communication example 103
point-to-LAN communication, example 102
point-to-point communication example 101
programs described 97
providing 97
remote control programs described 97

Remote Access Service
See RAS
remote nodes
configuring 49
Report command
File menu 40
requirements
iFIX hardware 4
iFIX software 7
memory 6
restricting access to SCADA servers 106
restricting database write access 107
routing application messages 57
running iFIX as a service 47
user account for 47
running iKeyDiag 22
run-time
error codes 125

S

SAC 86
alarm condition detection 93
controlling startup status 63
viewing information 88
SCADA server failover
enabling database access for 108
grouping SCADA Servers 45
logical node names 110
SCADA servers
configuring 49, 60
configuring failover 110
enabling support 60
grouping 45
polled by objects in an operator display 92
restricting access to 106
SCU 1
advanced alarm configuration functionality 57
configuring tips 37
exiting 39
implementing in iFIX, list of general tasks 43
main window 38
opening a new file 40
report described 40
starting 37
switching from NetBIOS to TCP/IP 34
SCU file
adding a file description 40
creating a report 40
described 2
naming 40
operations 39
read by iFIX Startup program 77
specified file not found 40
specifying name 45
SCU toolbox
Network button 48, 49
Security button 48
Task button 62
security
configuring 48
Security button
SCU toolbox 48
Security Configuration program
configuring security 48
service under Windows
running iFIX as 47
session timers
configuring 96
determining values 95
function 95
sessions
network 91
problems establishing or losing 116
temporary loss 94
working with configurable timers 94
setup
NetBEUI 26
network overview 25
TCP/IP 29, 31
sharing information among computers 48
Show History
startup option 81
shutdown
iFIX 81
software requirements
iFIX 7
SQL 86
configuring service 66
viewing statistics 88
starting SCU 37
Startup
program iFIX 77
startup
automatic, I/O drivers 64
configuring tasks 62
controlling status of SAC 63
error messages 124
iFIX 77
startup options
iFIX 80
Startup Queue Configuration
enabling 56
supported
file servers 11
network software 11
networks 10

T

Task button
SCU toolbox 62
TCP/IP
configuring 29
enabling in the SCU 34
establishing communication using 48
interface provided by RAS 98
mapping IP addresses 29
required components 28
troubleshooting 121
using 28
TCPTEST
using to troubleshoot TCP/IP 122
THISNODE placeholder
sharing information among computers 48
timers
session configurable 94
troubleshooting
Auto Alarm Manager 126
avoiding problems 114
computer components 114
computer failures 115
memory management 113
Microsoft networking 118
multi-tasking 113
NetBIOS with NBTEST 118
network error codes 124
networks 117
possible causes of problems 113
run-time error codes 125
startup error messages 124
TCP/IP 121

U

updates to links in displays 92
USB hardware key 16
USB port hardware key 16
user accounts
for iFIX running as a service 47
required group membership 3
using iKeyDiag 22

V

verifying port assignments 31
video drivers
recommended 9
virtual memory configuration, optimizing for iFIX 24

W

Wide Area Networks (WANs)
working with 96
Windows
optimizing virtual memory 23
running iFIX as a service under 46
Windows registry
editing the 2000 RAS server 100
editing the NT RAS server 100
specifying names 45
Windows service
running iFIX as one 47